CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

VÍCTOR HUGO GIRÓN MICOLTA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTANDER DE QUILICHAO
2021

CAPACIDADES TÉCNICAS, LEGALES Y DE GESTIÓN PARA EQUIPOS BLUE TEAM Y RED TEAM

VÍCTOR HUGO GIRÓN MICOLTA

SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM

JOHN FREDDY QUINTERO TAMAYO
DIRECTOR DE CURSO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SANTANDER DE QUILICHAO
2021

TABLA DE CONTENIDO

TABLA DE FIGURAS

RESUMEN

El avance que ha experimentado el sector informático en el transcurrir de los años ha sido exponencial, con el tiempo se puede determinar que las nuevas tecnologías de la información cada vez se insertan en los procesos de desarrollo o servicios dentro de las empresas para brindar un mejor servicio a toda una sociedad que busca satisfacer algún tipo de necesidad. Este tipo de necesidad son las que las compañías buscan analizar dentro de su comunidad para poder llegar de una forma clara y directa sin afectar sus principios, los cuales distinguen a la compañía, y para esto, se ciñen a normas y leyes que hacen que sus procesos tengan un cambio para bien, tanto para la misma compañía como para sus clientes.

En este caso los cambios vienen a reflejarse en el manejo de la información y los activos internos, los cuales hacen que una compañía tenga una identidad y también una buena funcionalidad en el sector en el que se desenvuelve, con esto logra tener un buen control de la información que es utilizada para bien de la misma compañía. Al hablar sobre la seguridad de la información, la cual es esencial y que está como norma o proceso necesario para aplicarlo dentro de la organización fortaleciendo de esta manera la misma, brindando estándares de seguridad a la información, esta hace referencia a la forma de cómo organizar y dar tratamiento a los datos, con ella se determinan los activos importantes que hay que proteger, las vulnerabilidades en que pueden estos activos verse involucrados en determinado momento y las amenazas que conllevan.

Es por esta razón de que existen formas de llevar a cabo la protección de la información organizacional, este es el caso de los equipos Red Team y Blue Team, los cuales desempeñan roles diferentes en el proceso de salvaguardar la información, el Rea Team lleva a cabo de forma controla todo lo relacionado a ataques simulados, pruebas de instrucción a los sistemas con el único fin de encontrar posibles fallas, vulnerabilidades y de esta manera implementar posibles soluciones al tipo de vulnerabilidad encontrada. Ahora el complemento de este equipo es el Blue Team el cual tiene como función implementar las medidas de defensas que hagan que blinden al sistema de posibles riesgos, y lo lleva a cabo haciendo vigilancia constante del sistema revisando los procesos que salen de él, de esta manera se busca tener control general de la infraestructura tecnológica.

GLOSARIO

Análisis de riesgos: El proceso de análisis y gestión de riesgos es uno de los elementos más importantes constituidos dentro del Sistema de Gestión de la Seguridad de la información por cuanto este análisis constituye una metodología para obtener la información sobre las vulnerabilidades, amenazas y los riesgos que forman el conjunto de elementos que crean el campo de falencias de la seguridad de la informática[1]

Probabilidad: Para determinar la probabilidad de ocurrencia es posible de la forma cualitativa o cuantitativamente, considerando que la medida no debe contemplar la existencia de acciones de control.

Amenazas: Son acciones que pueden generar consecuencias negativas en la operación de la organización. Se referencian como amenazas a las fallas, los ingresos no autorizados, los virus, los desastres ocasionados por fenómenos naturales o ambientales, etc.

Vulnerabilidades: Son ciertas condiciones a las que se exponen los activos, están presentes en su entorno, facilitan que las amenazas se materialicen y se conviertan en vulnerabilidad.

Activos: Los activos en tecnología, es todos lo relacionado con los sistemas de información, las redes las, comunicaciones y la información en sí misma.

Impactos: Son las consecuencias de la materialización de las distintas amenazas y los daños que éstas puedan causar. Las pérdidas generadas pueden ser financieras, tecnológicas, físicas, entre otras.

Diagnostico e identificación de los riesgos: Este proceso surge de la utilización de las herramientas o las metodologías apropiadas en las cuales se pueden encontrar la forma metódica para efectuar el análisis en base a la organización en la que se pretenda análisis en este sentido se tienen en cuenta tres variables fundamentales sobre las cuales se basa la operación de análisis: activos, las amenazas y las vulnerabilidades son el objeto para identificar los riesgos, dado que una brecha no detectada permite la entrada al sistema de posibles amenazas.[2]

Seguridad Informática: Comprende las características, condiciones y parámetros de los sistemas de procesamiento de información para su almacenamiento administración y gestión, garantizando su confidencialidad, integridad y disponibilidad. Considerar las características de seguridad informática significa conocer el riesgo clasificarlo y protegerse de los ataques y daños de la mejor forma

[1] Universidad nacional abierta y a distancia, Mirian del Carmen Benavides, Francisco Solarte. (2012). *Módulo riesgos y control informático.* Bogotá: Dátatela UNAD.

[2] GOMEZ, R. D. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*.

posible. Esto quiere decir que solamente cuando se conocen las potenciales amenazas, agresores y sus diferentes intenciones dañinas que pueden ser directas o indirectas en contra de un sistema o una organización, se puede adoptar las medidas de protección adecuadas, para que no se vulneren los recursos de información valiosos. En otros conceptos representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información.[3]

Pilares de la seguridad Informática: Se busca proteger en la información, son los cuatro pilares importantes que conlleva a que la información sea resguardada a gran escala. A continuación, se especifican en su orden:

Confidencialidad: La información sólo puede y debe ser accedida, utilizada y gestionada por el personal de la empresa que ha obtenido la autorización para hacerlo. Se considera que este tipo de información no debe ser revelada a personal ajeno, ni debe ser pública, por lo tanto, debe ser protegida por su razón de ser y sus características.[4]

Integridad: Se refiere al momento en que la información de ninguna forma ha sido borrada, copiada o modificada, es decir, cuando se conserva tal como fue creada o enviada desde cualquier medio desde su origen hacia su destino. Un ataque a la integridad de la información se puede presentar en archivos planos de bases de datos, información documental, registros de datos, etc.[5]

Disponibilidad: Tiene que ver con que la información facilitada en cualquier medio digital o software se encuentre a disposición de un usuario autorizado para el procesamiento de los datos, para el correcto funcionamiento de una organización, así como de sus clientes o personal requerido sin que estos sean afectados.[6]

Autenticidad: Este pilar se define aquella información legítima, que, al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica.[7]

Equipo Blue Team: Expertos en seguridad informática que buscan defender a entidades de ataques realizados por delincuentes cibernéticos.

---

[3] RAULT, A. -M.-S.-N.-R.-F.-J.-S.-D.-R. (2010). SeguridadInformática - Ethical Hacking. Ediciones ENI.

[4] Confidencialidad.
https://books.google.es/books?id=Mgvm3AYIT64C&dq=integridad+seguridad+informatica&lr=&hl=es&source=gbs_navlinks_

[5] Integridad. Seguridad informática. Autor: Purificación Aguilera López.Editex, 2010 - 240 páginas.
https://books.google.es/books?id=Mgvm3AYIT64C&dq=integridad+seguridad+informatica&lr=&hl=es&source=gbs_navlinks_

[6] Disponibilidad. Seguridad informática. Autor: Purificación Aguilera López.Editex, 2010 - 240 páginas.
https://books.google.es/books?id=Mgvm3AYIT64C&dq=integridad+seguridad+informatica&lr=&hl=es&source=gbs_navlinks_

[7] Autenticidad. http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServAutenticacion.php

Equipo Red Team: Expertos en seguridad informática, que se dedican a simular ataques controlados a los sistemas para la explotación de vulnerabilidades y saber cómo contrarrestarlos.

INTRODUCCIÓN.

La seguridad de los bienes informáticos se ha convertido en algo primordial hoy en día, el avance de la tecnología está acompañado de una serie de riesgos o amenazas que pueden ser detectados y reducidos mediante una buena implementación en la seguridad de la información, ya que estos se pueden determinar mediante planteamientos y análisis de riesgo, como qué tipo de información debemos proteger, de qué la protegemos, cuáles son las posibles amenazas, implementación de medidas de control y mecanismos que protejan la información, sin que estas acciones incrementen los gastos, su efectividad será medible en el seguimiento realizado cada vez que sea encontrada una debilidad.

Cada vez las organizaciones buscan la forma, la manera de proteger sus activos, se han dado cuenta de que hoy en día la información que ellas manejan juegan un papel fundamental en el ciclo de vida de la misma compañía y de su reputación, y en estos tiempos aún más ya que el crecimiento de la tecnología a nivel mundial ha hecho que pequeñas empresas incursionen en el mundo tecnológico, y deben entender que para un buen manejo de la tecnología hay que también saber protegerse de un medio el cual es nuevo para muchas de ellas.

Ahora bien, dentro de las organizaciones deben contar con los recursos necesarios, personal idóneo en el manejo de riesgos y vulnerabilidades cibernéticas, políticas y procedimientos que determinen un buen manejo de riesgos sobre sus activos de información, el contar con esto ayuda a darle mejor estabilidad a las compañías con respecto a sus funciones operativas, logrando que no sufra mucho daño al momento que ocurra un determinado ataque cibernético, y sobre todo que el abordar estos incidentes se hagan de una manera rápida pues para las organizaciones el tiempo es prioridad para que sus operaciones no se detengan y puedan seguir prestando sus servicios de acuerdo a su entorno de mercado.

1. OBJETIVOS.

1.1. OBJETIVO GENERAL

- Realizar un informe técnico en el cual se muestren las estrategias para el análisis de riesgos y vulnerabilidades en una infraestructura tecnológica planteas en las etapas del Seminario Especializado, Equipos Estratégicos en Ciberseguridad: Red Team & Blue Team Código: 202337164.

1.2. OBJETIVOS ESPECIFICOS

- Evaluar las acciones de los equipos Red Team & Blue Team de una organización en el marco de los criterios éticos y legales.

- Realizar un análisis de las implicaciones éticas y dilemas morales.

- Demostrar vulnerabilidades en un sistema informático a partir del uso de metodologías y técnicas de intrusión.

- Formular estrategias de contención mediante el análisis de riesgos y vulnerabilidades en una infraestructura TI.

2. DESARROLLO DEL INFORME

2.1. MARCO LEGAL.

Consultando la documentación que existe en nuestro país con respecto a las leyes de la seguridad de la información y protección de esta, podemos mencionar que existen distintos artículos que hacen referencia a la protección de la información en el campo de las telecomunicaciones, en este citamos algunos de los artículos que hacen mención a ello y que se encuentran en la legislación y normatividad de la Ley No. 1273 del 5 de enero de 2019 "POR MEDIO DE LA CUAL SE MODIFICA EL CÓDIGO PENAL, SE CREA UN NUEVO BIEN JURÍDICO TUTELADO - DENOMINADO "DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS"· Y SE PRESERVAN INTEGRALMENTE LOS SISTEMAS QUE UTILICEN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENTRE OTRAS DISPOSICIONES". Este es una de tantas leyes que existen y que nos ayuda a realizar un control en cuanto al tráfico de información digital.

En ella se mencionan varios artículos que pueden ser aplicar en la alteración de información, manipulación y distribución de datos confidenciales. Teniendo presente lo anterior y las personas que realicen prácticas indebidas con la manipulación de información perteneciente a entidades públicas o privadas le podrían aplicar los siguientes artículos contenidos en la Ley No. 1273 del 5 de enero de 2019 y los cuales son:

ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTÍCULO 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

ARTICULO 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y cho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Ahora demos un vistazo al DECRETO 1377 DE 2013, Ley1581 de 20122, es una ley que se promulgo el 27 de junio de 2013 y que propende en todo lo relacionado con la protección de los datos personales de los individuos de nuestro país, en ella se establecen distintas facetas que tienen que ver con los datos, como estos se procesaran o manejaran por entidades públicas o privadas, saber qué tipo de información será publica o en su defecto no se podrá manipular o deberá tener permiso para ello.

Esta ley es tan importante que es por medio de ella en la que nosotros los individuos podremos estar enterado de que es lo hacen con nuestros datos, cual es la manipulación de estos, que se hacen con ellos y como es la forma en que estos son recolectados. Si logramos ver, todas las entidades que incursionan en el mundo digital, sus sistemas de manipulación y tratamiento de información están puestos en los sistemas virtuales, que hoy son el día a día de las instituciones y por donde, en muchas ocasiones llegan a las personas y es por ello se debe tener presente todas estas leyes, artículos que en ella se encuentran para que de esta forma sepamos darle importancia a los datos privados y públicos, sepamos en qué momento son propio su tratamiento.

A continuación, se mencionan algunos artículos que son importantes tener muy presentes para el manejo de la información personal:

Artículo 3°. Definiciones. Además de las definiciones establecidas en el artículo 3° de la Ley 1581 de 2012, para los efectos del presente decreto se entenderá por:

1. Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

2. Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

3. Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

4. Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

5. Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

Artículo 4°. Recolección de los datos personales. En desarrollo de los principios de finalidad y libertad, la recolección de datos deberá limitarse a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente. Salvo en los casos expresamente previstos en la ley, no se podrán recolectar datos personales sin autorización del Titular

Artículo 5°. Autorización. El responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de estos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

2.2. PRUEBAS DE PENETRACIÓN O PENTESTING.

Revisando un poco lo que permite el sistema de Pentesting vemos que nos sirve para realizar un ataque controlado dentro de un sistema de redes de informática, al cual le necesitamos revisar si existen vulnerabilidades o se puedan presentar, de esta forma sabremos cómo se comportan dichos sistemas, como podrían ser atacados, y como podríamos defendernos. Las etapas que nos muestra esta técnica son pertinentes para abordar dicho ataque simulado y las cuales vamos a describir a continuación:

- Etapa de información: Esta es la etapa inicial de proceso de simulacro, en la que se tiene relación con el personal de la empresa, quien nos proveerá la información necesaria para la prueba, en ella se definirá el alcance que va a tener, que procesos del sistema se van a revisar, que equipos, direcciones o rangos de IP.

- Etapa de búsqueda de vulnerabilidades: En esta etapa se verifica de acuerdo con la información que se obtuvo, por donde se pueden presentar las vulnerabilidades dentro del sistema, cuales procesos están más expuestos a ello y así poder tomar medidas claras y efectivas. Por

ejemplo, se puede presentar fallos en como los usuarios utilizan los servicios de autenticación en las aplicaciones de la organización.

- Etapa de explotación de vulnerabilidades: Aquí es donde se ejecutan ciertas aplicaciones dentro de los sistemas de información de la organización, en las que se ponen a pruebas las vulnerabilidades encontradas, con ello se podrá determinar si por ejemplo hay sistemas que no cuentan con sistema de Login, sería una identificación de vulnerabilidad del sistema.

- Etapa de Post-explotación: Una vez explotadas las vulnerabilidades en esta etapa se busca llegar más afondo más lejos dentro del mismo sistema, pero siempre y cuando se cuente con los privilegios necesarios para ello y se tenga los permisos.

- Etapa del Informe: En la etapa final es donde se documenta todo lo realizado en el proceso realizado dentro de la organización en la búsqueda de vulnerabilidades y su puesta a prueba, se identifican y se da el resultado final, en dicho informe se especifican cuáles son las vulnerabilidades más críticas, como se deben tratar para así poder corregirlas y que el sistema de dicha empresa no se vea afectado en un futuro, se muestra también cuales tienen un buen sistema de seguridad.

2.3. HERRAMIENTAS DE CIBERSEGURIDAD.

- Metasploit: Es una herramienta con la cual se puede llegar a identificar los posibles fallos de un sistema, permite la explotación de vulnerabilidades, que tan grabe es dicha vulnerabilidad y muestra lo expuesto que estaría un sistema, se puede llegar a robar información por medio de esta herramienta, interrumpir software como lo es un antivirus entre otras opciones.

- Nmap: Es una herramienta que permite el análisis de un sistema de red, en la cual se llega obtener información como lo es que equipos están conectados, que puertos se encuentran abiertos, direcciones IP p MAC, se puede determinar los servicios que están corriendo y cuáles pueden ser afectados en un ataque.

- OpenVas: Es un paquete de software el cual cuenta con distintas herramientas con las cuales se llega a analizar un sistema de red de datos, conocer puertos abiertos, distintas vulnerabilidades, que aplicaciones están activas.

Servicios en línea:

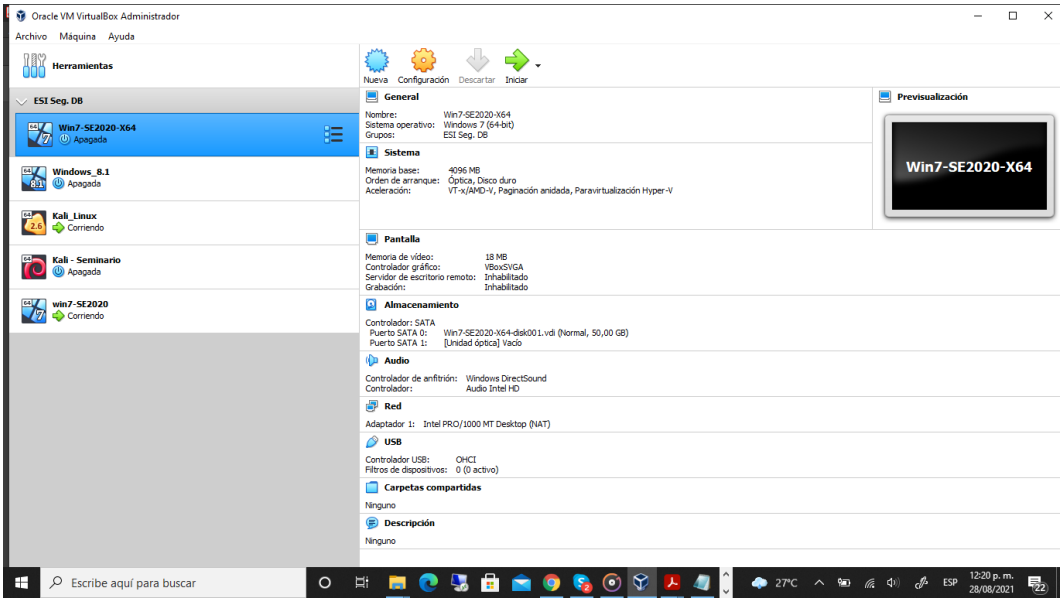
- ExploitDB: Este es un servicio en donde mucha gente interesada en la seguridad de la información con respecto a las vulnerabilidades de los sistemas socializa dichas vulnerabilidades para luego si alguien desea instruirse en ella lo puede hacer.

- CVE: Es un sistema web en el cual se almacena y codifica todas las fallas y vulnerabilidades que se presentan en el campo de la informática, en este lo que se hace es codificar dichas fallas para así tenerlas identificadas y poder saber de una forma muchas más rápida el tipo de vulnerabilidad que se está tratando por parte del personal de seguridad.

  Estos dos servicios en línea o dentro de web son muy importantes, ya que con ellos se pude estar documentando constantemente de las vulnerabilidades que aparecen día a día en los sistemas informáticos, nos brindan una guía de cómo tratarlos, algo muy importante es que esto se debería realizar con el ánimo de hacer el bien no para dañar la idea es ayudarnos para así fortalecer los sistemas que manejemos en un futuro, pues debido a la facilidad de conseguir la información le mente en ocasiones de las personas cambian de rumbo cuando se despierta la maldad y más aún cuando se tiene alguna recompensa por delante.

3. CONFIGURACIÓN DEL BANCO DE TRABAJO PARA LAS PRUEBAS DE PENETRACIÓN.

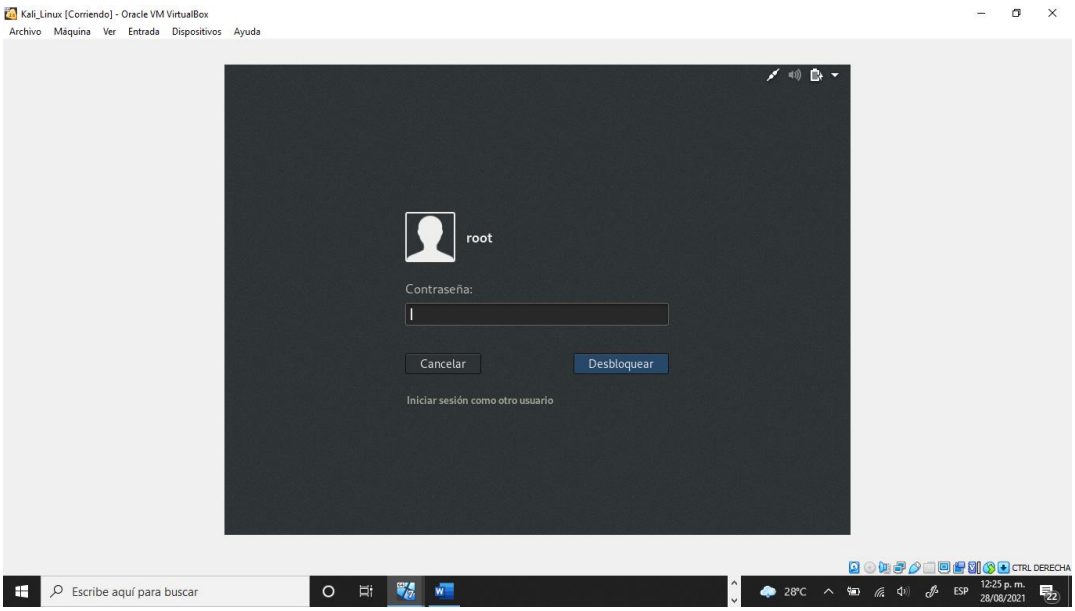
Figura 1: Panel de VirtualBox.



Fuente: Propiedad del autor.

Se inicia la máquina de Kali Linux, en este caso inicio una máquina la cual descargue la imagen ISO (kali-linux-2019.3-amd64), ya que la que se nos dieron para el diplomado esta solicita un usuario y contraseña el cual no lo tengo en él momento, por esta razón instale otra máquina de Kali Linux para demostrar la comunicación con las otras máquinas de Windows 7.

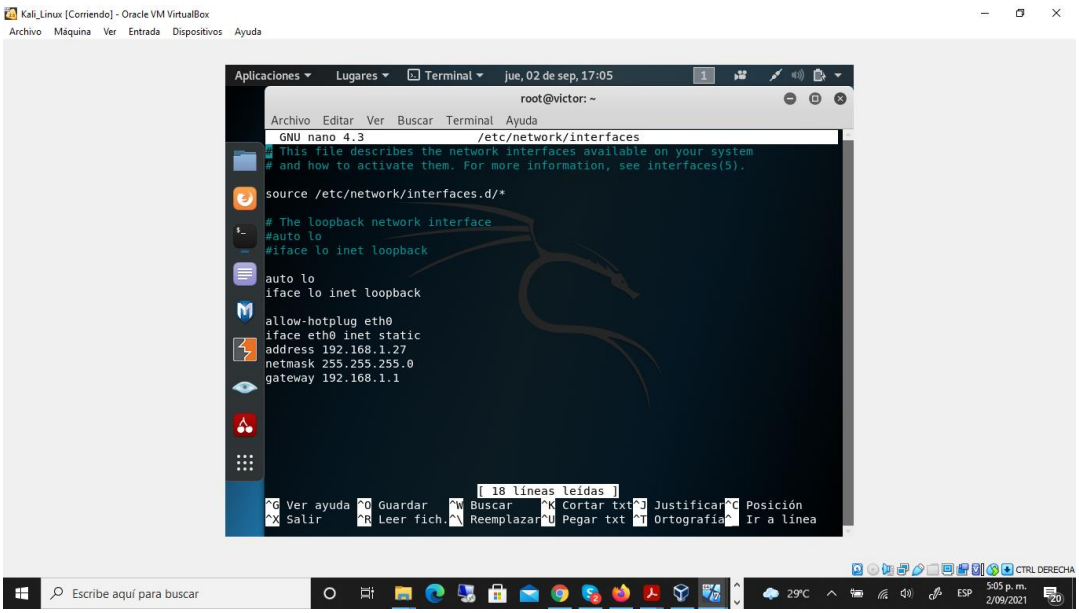
Figura 2: Acceso a la Máquina Kali Linux.



Fuente: Propiedad del autor.

Se acceden a las configuraciones de red de la máquina de Kali Linux y asignamos de forma manual la dirección IP: 192.168.1.27

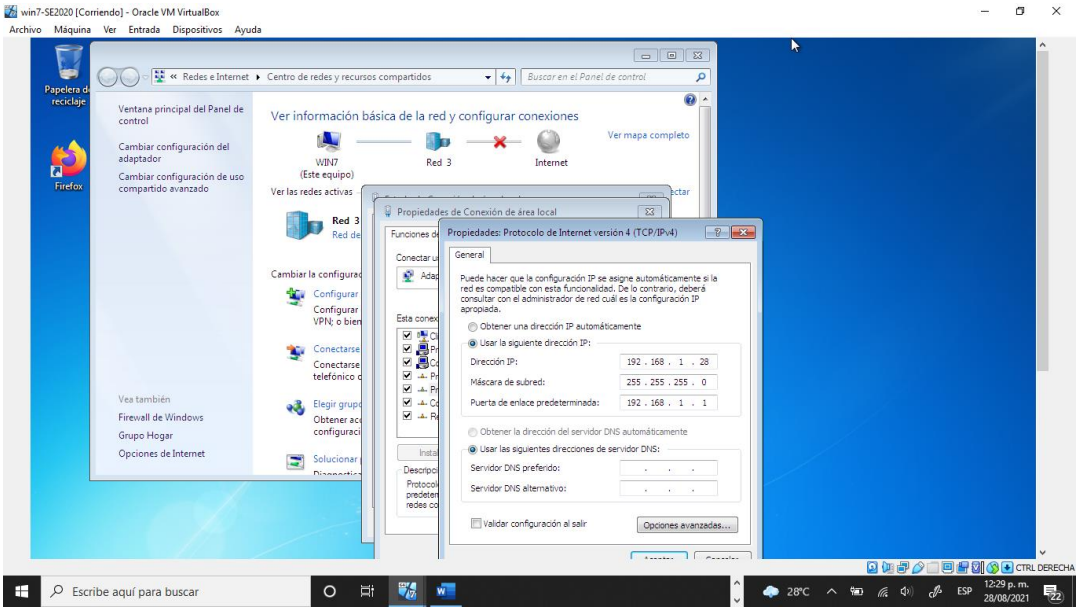
Figura 3: Configuración de tarjeta de red en Kali Linux.



Fuente: Propiedad del autor.

Ahora se inicia la máquina de Windows 7 “wind7-SE2020” y asignamos también una dirección IP de forma estática la cual será la 192.168.1.28

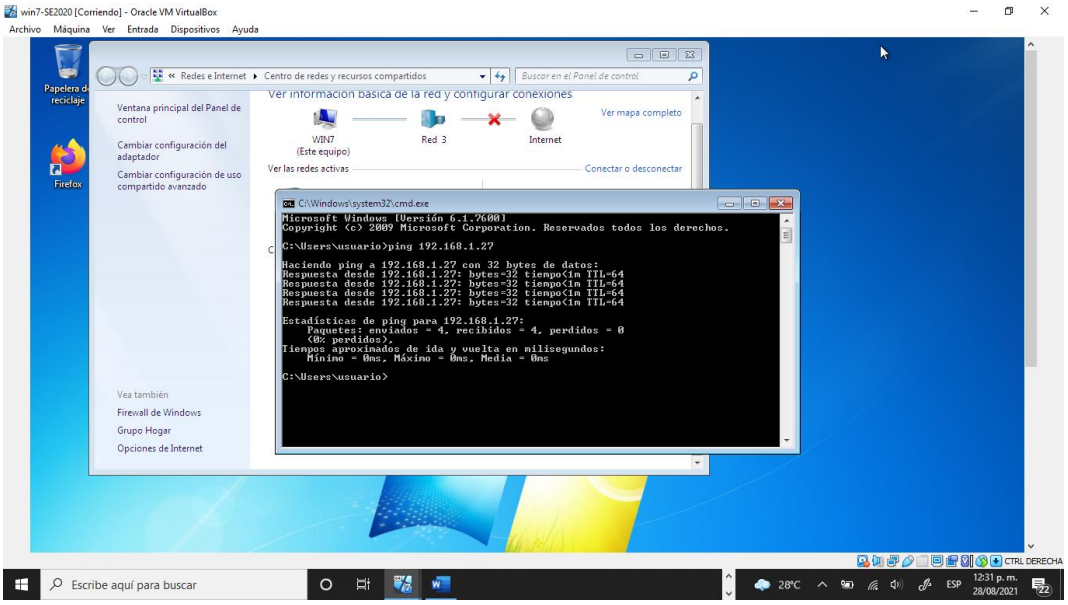
Figura 4: Configuración de tarjeta de red en Windows 7“wind7-SE2020”.



Fuente: Propiedad del autor.

Realizamos un ping para establecer comunicación entre estas dos máquinas, primero desde Windows 7 y luego desde Kali Linux.

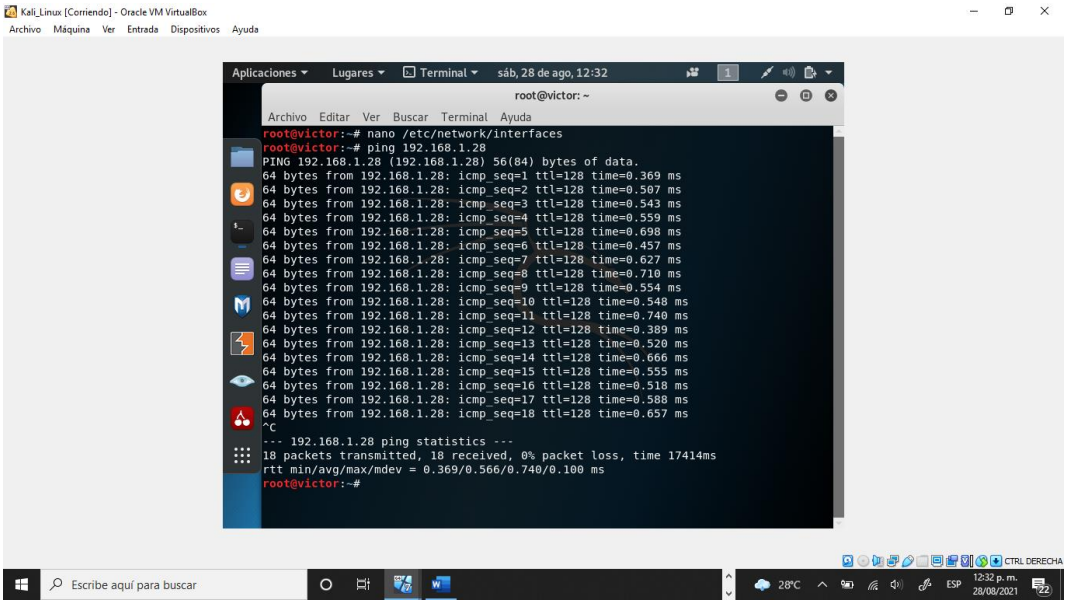
Figura 5: Comunicación entre Windows 7“wind7-SE2020” y Kali Linux.



Fuente: Propiedad del autor.

Desde Kali Linux:

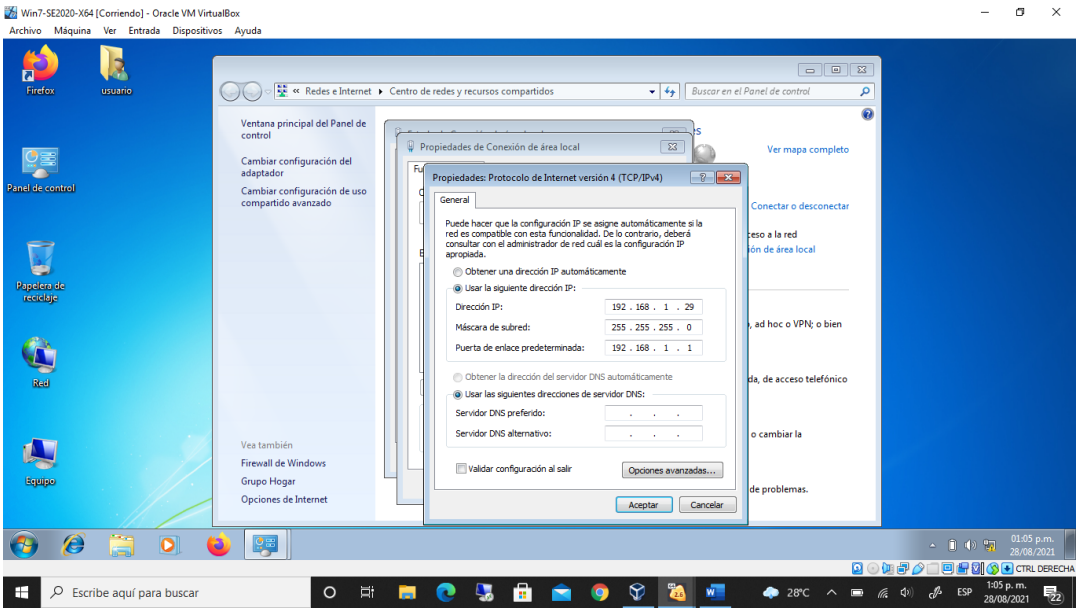
Figura 6: Comunicación entre Kali Linux y Windows 7“wind7-SE2020”.



Fuente: Propiedad del autor.

Abrimos la segunda máquina que tiene instalado el sistema operativo Windows 7 “Win7-SE2020-X64”, y le asignamos la dirección IP 192.168.1.29.

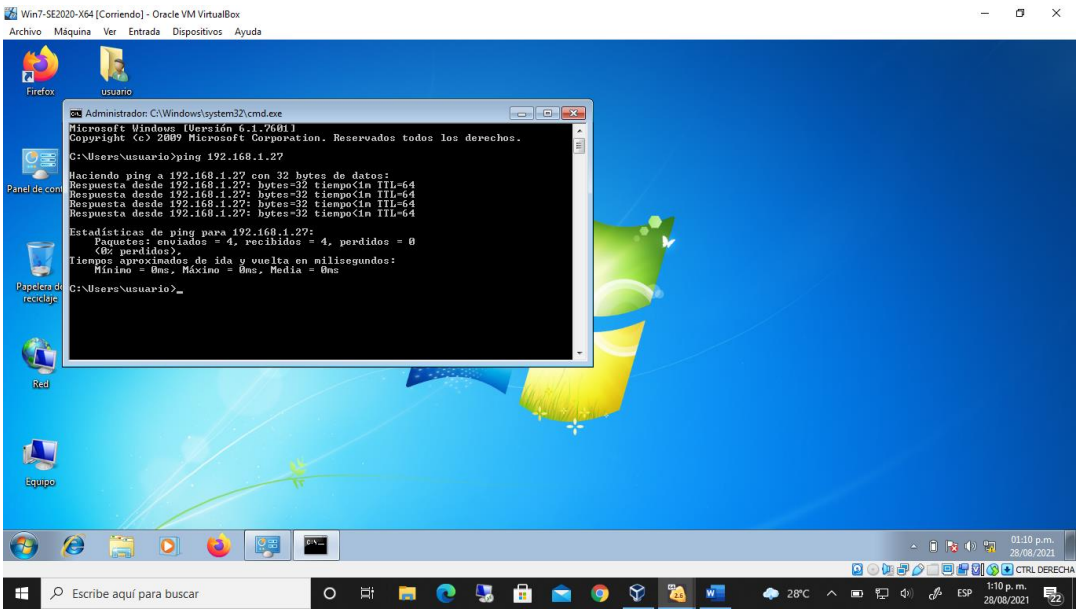
Figura 7: Configuración de IP en Windows 7 “Win7-SE2020-X64”



Fuente: Propiedad del autor.

Se realiza el proceso de conexión de esta máquina virtual Win7-SE2020-X64 con la máquina de Kali Linux por medio de un ping.

Figura 8: Conexión de Windows 7 “Win7-SE2020-X64” y Kali Linux.



Fuente: Propiedad del autor.

De esta forma se evidencia que hay conexión entre las tres máquinas virtuales Kali Linux y las de Windows 7 “wind7-SE2020” y “Win7-SE2020-X64”.

4. CONSIDERACIONES ETICAS.

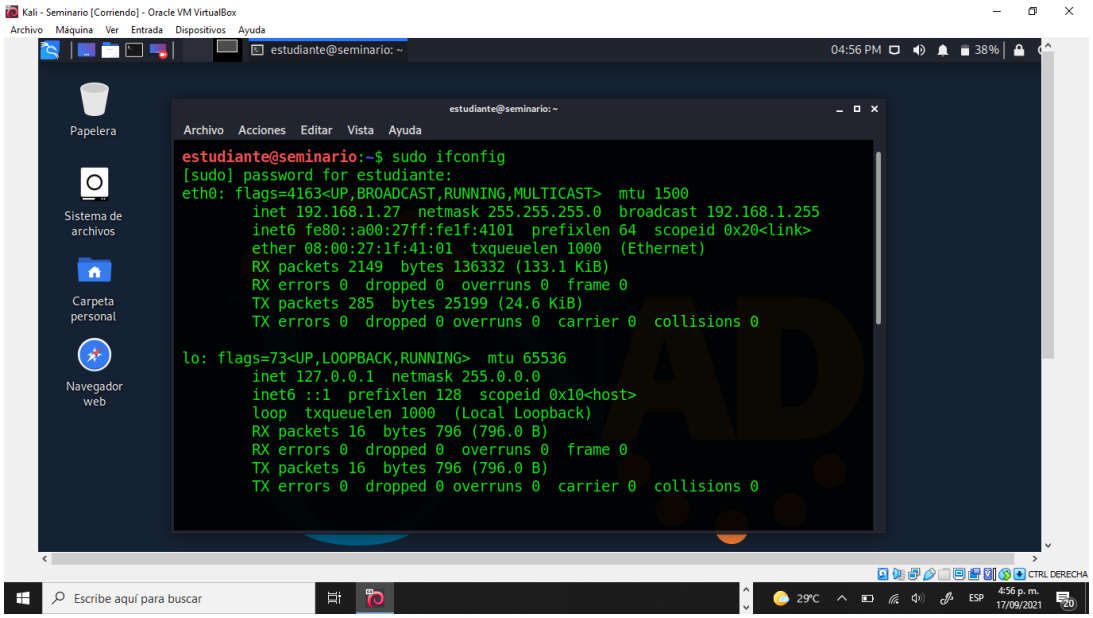
El código de ética para ingenieros es muy claro en todas sus cláusulas para el ejercicio del cumplimiento de las funciones de un ingeniero en determinada empresa sea pública o privada, y si lo detallamos en su totalidad se logra ver que aceptar ese empleo con “The WhiteHouse”. En el siguiente Artículo 34 del código de ética es muy claro lo que dice, que sin duda al leerlo nos dice que actuar de manera trasparente ante los cargos adquiridos es un deber y que no debe estar primero el interés propio al del beneficio de toda una sociedad. [8]*ARTÍCULO 34. PROHIBICIONES ESPECIALES A LOS PROFESIONALES RESPECTO DE LA SOCIEDAD. Son prohibiciones especiales a los profesionales respecto de la sociedad: a) Ofrecer o aceptar trabajos en contra de las disposiciones legales vigentes, o aceptar tareas que excedan la incumbencia que le otorga su título y su propia preparación.*

[8] Copnia. (2015). Código de Ética para el ejercicio de la Ingeniería en general y sus profesiones afines y auxiliares. Copnia. (pp. 3-26). Consultado el 27 de agosto de 2021. Disponible en: https://www.copnia.gov.co/tribunal-de-etica/codigo-de-etica

5. EJECUCIÓN PRUEBAS DE INTRUSIÓN.

Para determinar conexión de las máquinas virtuales de Kali Linux con la de Windows 7 verificamos las direcciones IP que estén en la mi red de datos. La máquina de Kali Linux tiene la IP: 192.168.1.27

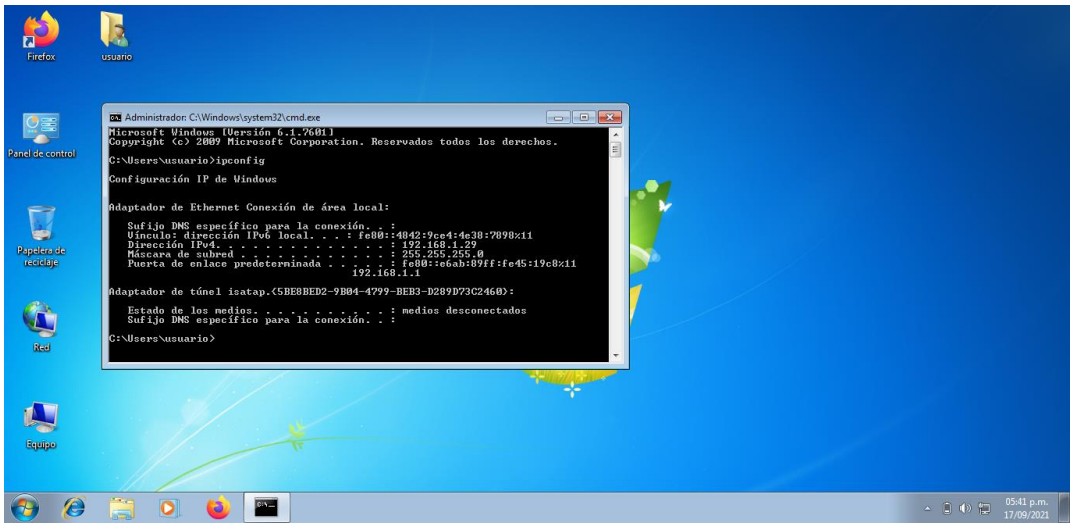
Figura 9: Consulta de la dirección IP de la maquina Kali Linux.



Fuente: Propiedad del autor.

Se observa la dirección IP del sistema operativo Windows 7 de 64 bits, la cual corresponde a IP: 192.168.1.29

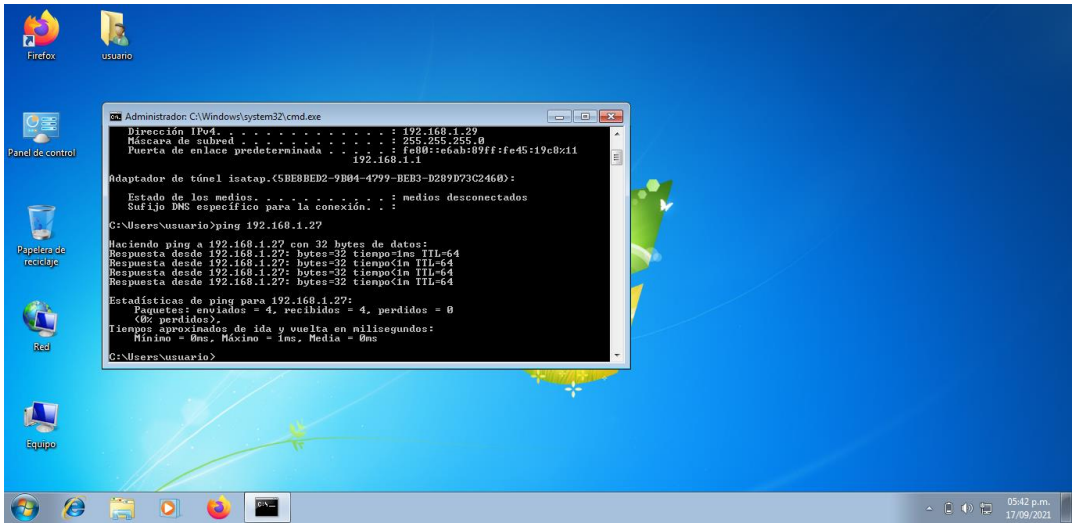
Figura 10: Consulta de la dirección IP de la maquina Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Se realiza la conexión con las dos máquinas anteriores por medio del comando ping a la dirección 192.168.1.27 del sistema Kali Linux.

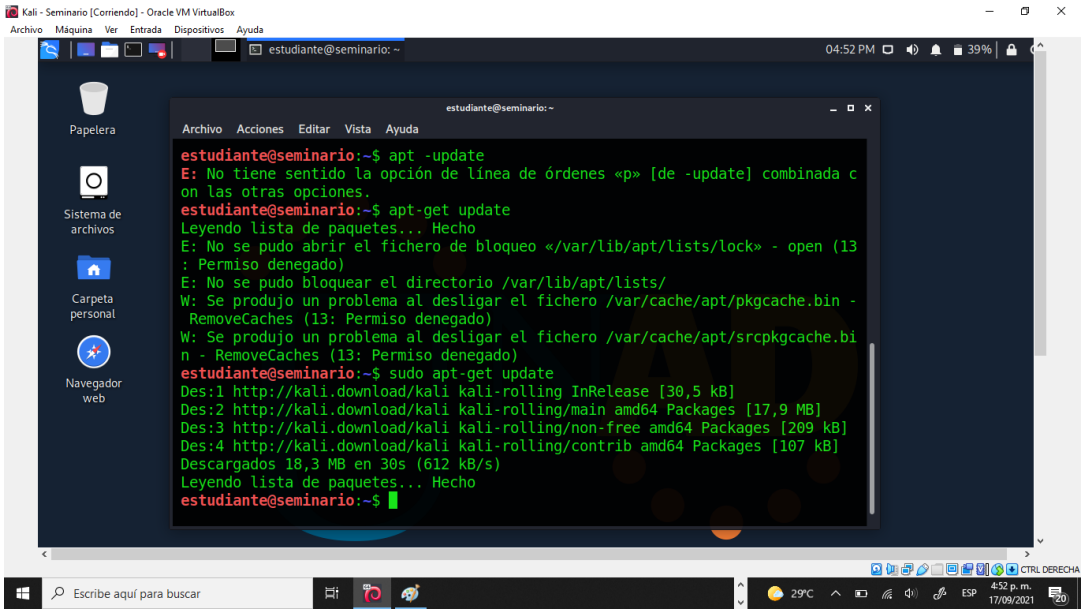
Figura 11: Conexión de la maquina Windows 7 de 64 bits con Kali Linux.



Fuente: Propiedad del autor.

Se efectúa el proceso de actualización de las aplicaciones que contiene Kali Linux en las versiones más recientes.

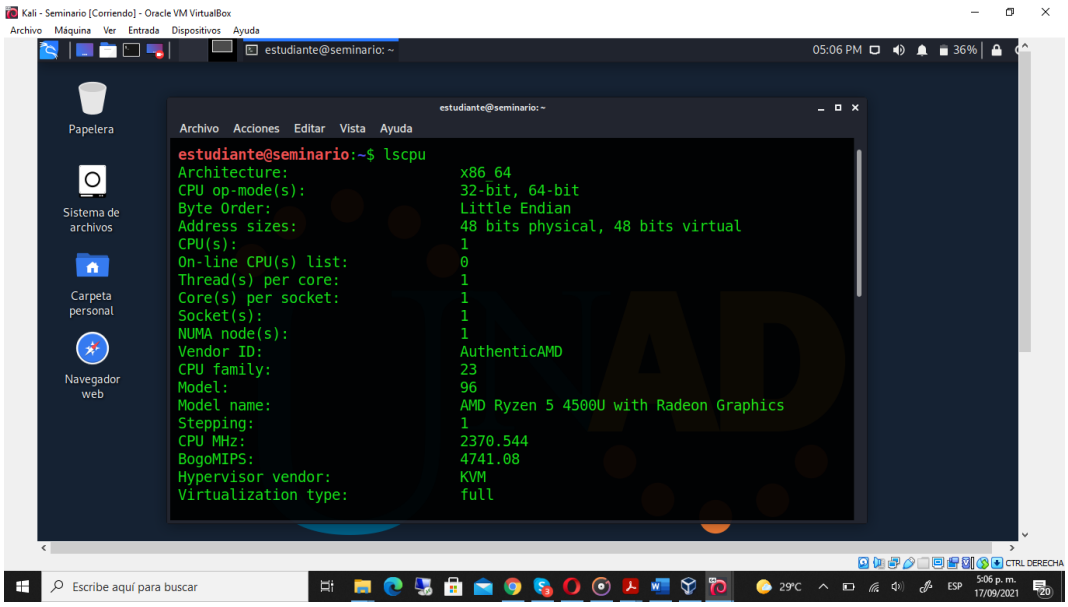
Figura 12: Actualización de los paquetes de Kali Linux.



Fuente: Propiedad del autor.

Con la siguiente imagen se ven las características técnicas de la máquina de Kali Linux la cual se usará para las pruebas de penetración que en este caso se utilizará la maquina suministrada por el director del diplomado:

Figura 13: Características técnicas de la máquina de Kali Linux.

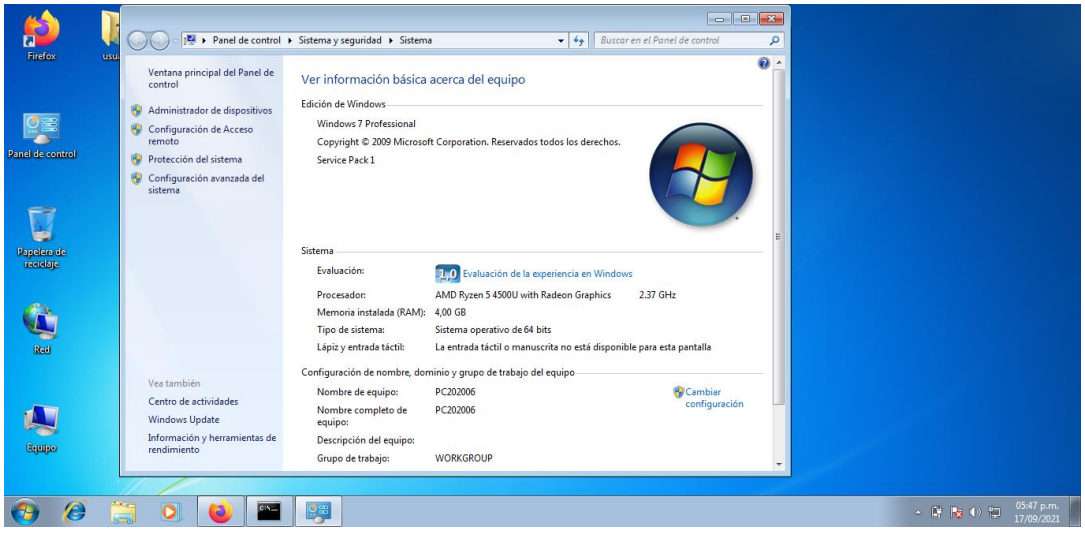


Fuente: Propiedad del autor.

Dentro de la máquina de Windows 7 de 64 bits, se procede a instalar la aplicación rejetto v. 2.3 para realizar el análisis de la información, determinar la fuga de esta.

Se observa la arquitectura del sistema operativo de Windows 7:

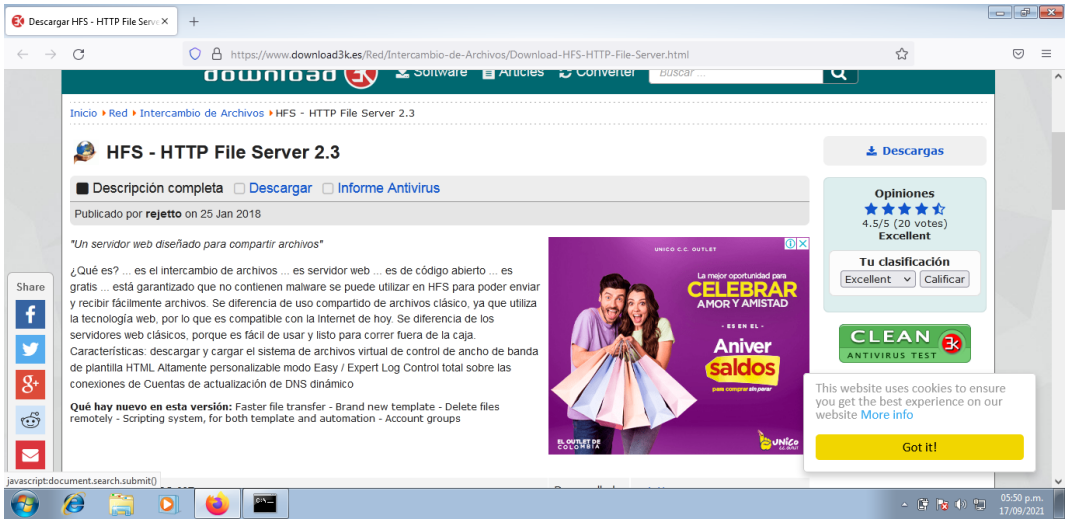
Figura 14: Características técnicas de la máquina de Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Determinamos la página web donde descargaremos la aplicación y luego procederemos a instalación en este sistema de Windows 7.

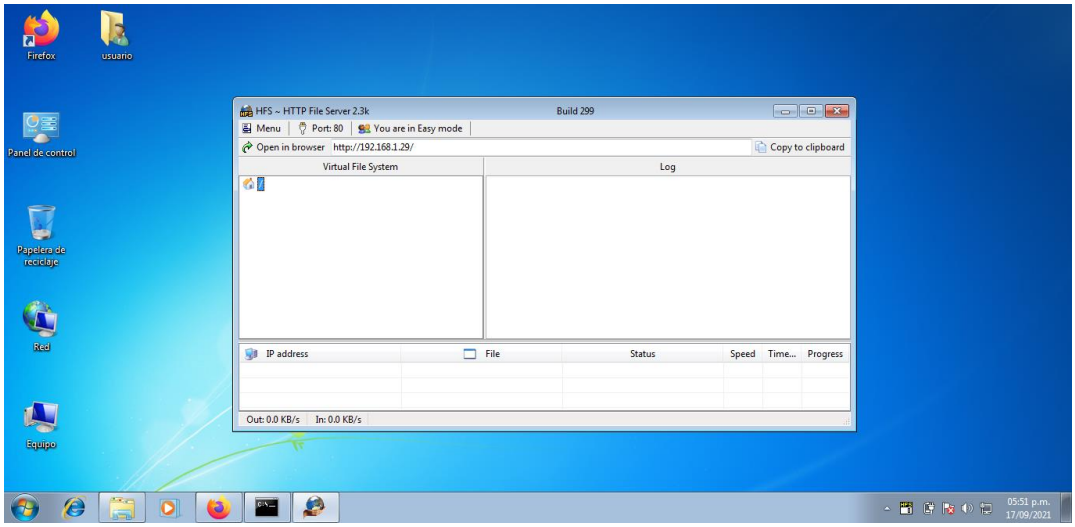
Figura 15: Descarga de la aplicación “rejetto v. 2.3”



Fuente: Propiedad del autor.

Instalación en la máquina de Windows 7 de la aplicación que presenta la fuga de información “rejetto v. 2.3”.

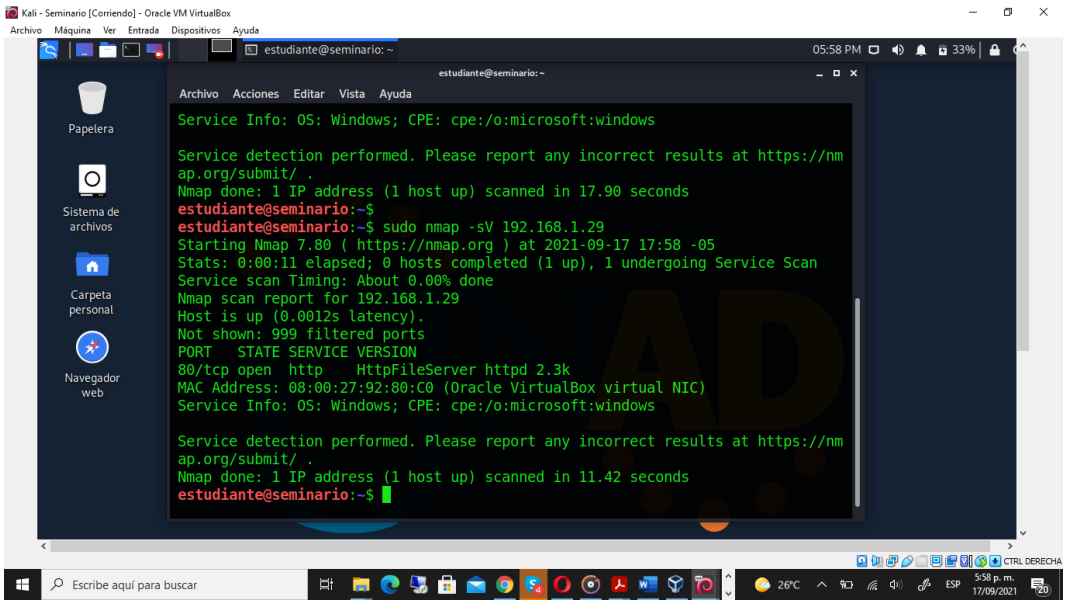
Figura 16: Aplicación “rejetto v. 2.3” instalada en Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Ahora por medio de la herramienta de análisis de puertos que posee el sistema de Kali Linux, se llevara a cabo el análisis de posibles vulnerabilidades que podemos encontrar en la maquina Windows 7 de 64 bits.

Figura 17: Escaneo de puertos de la maquina Windows 7 de 64 bits.

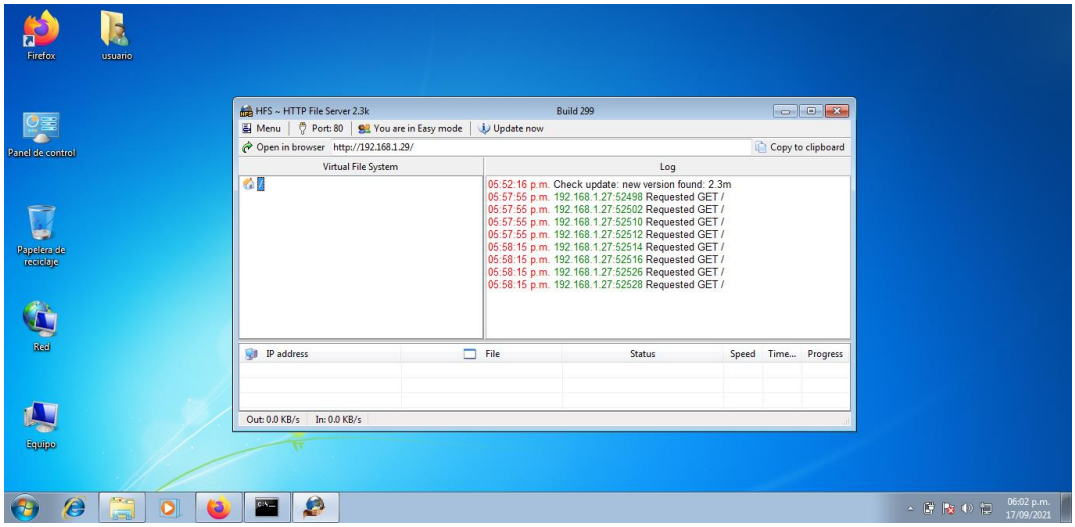


Fuente: Propiedad del autor.

Se observa por medio de Nmap que existe una vulnerabilidad referente al programa que se acaba de instalar en la máquina de Windows 7, el “HtttpFileServer” en la versión 2.3, el cual está abriendo el puerto 80/TCP.

En la siguiente imagen se plasma la operación del proceso realizado desde Kali Linux cuando se realizó el análisis de vulnerabilidades en la máquina de Windows 7.

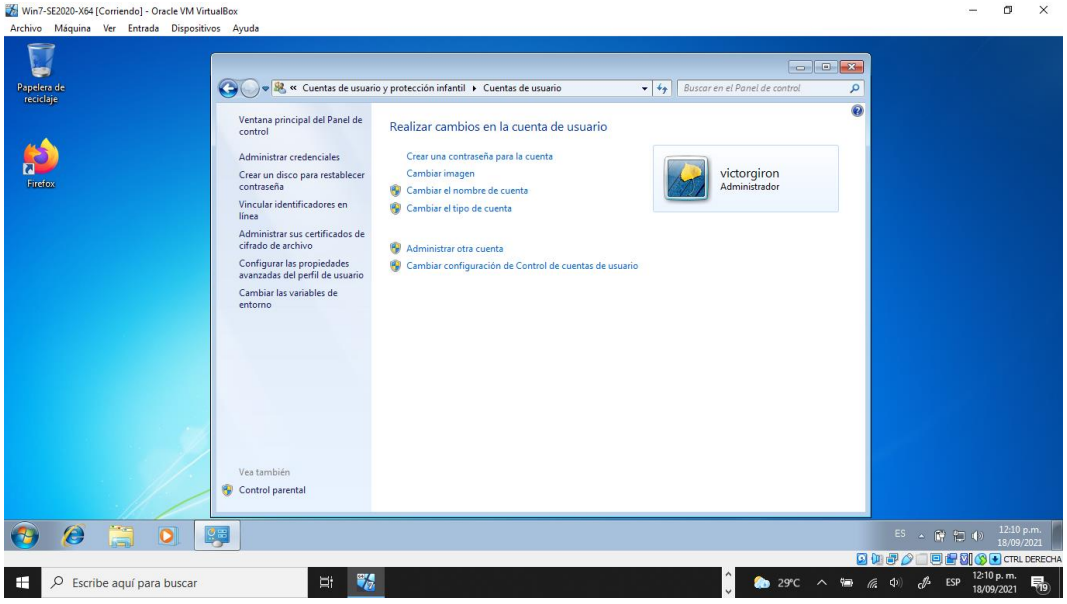
Figura 18: Ejecución de la aplicación “rejetto v. 2.3” en Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Creación del usuario administrador para demostrar la explotación de la vulnerabilidad encontrada. Procedo a crear también una cuenta distinta a la de estudiante dentro del sistema de Kali Linux con mi nombre y apellido “victorgiron” para realizar el ataque:

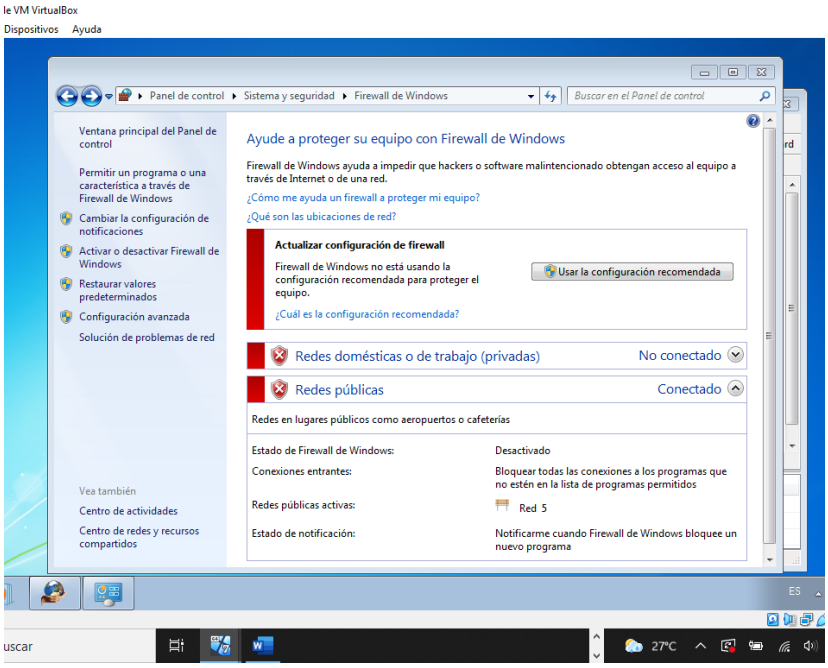
Figura 19: Creación de usuario administrador en Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Se a verificar que la seguridad de la máquina de Windows 7 de 64 bits, y se procede a desactivar el firewall.

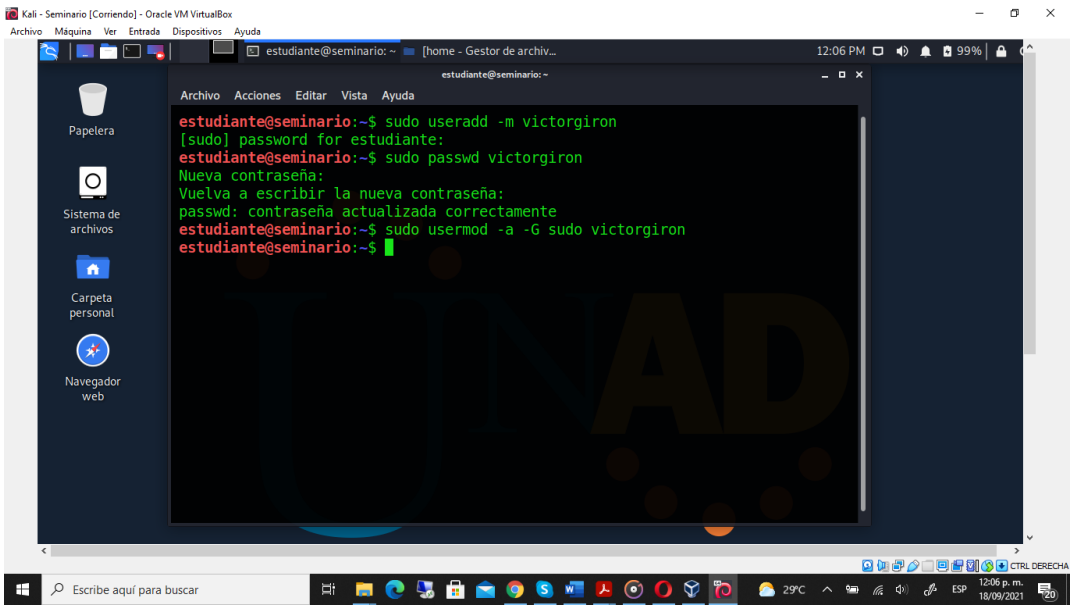
Figura 20: Firewall detenido en Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Dentro de la máquina de Kali Linux también se procede a crear una cuenta de usuario para trabajar distinta a la de estudiantes, esta será con el nombre de “victorgiron”.

Figura 21: Creación de usuario en Kali Linux.

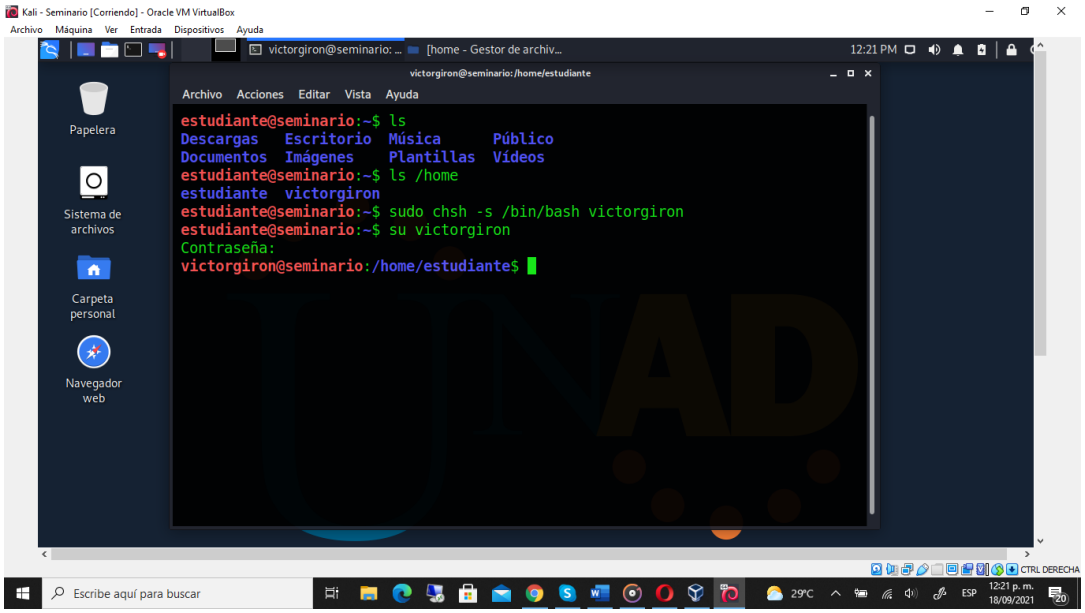


Fuente: Propiedad del autor.

Al crear el usuario damos una contraseña, y lo colocamos en el grupo de SUDO “sudo usermod -a -G sudo victorgiron”, para que tenga privilegios de administrador y poder realizar operaciones de administrador.

Agregamos el usuario al Shell para poder visualizarlo en el terminal con la siguiente instrucción: “chsh -s /bin/bash victorgiron”

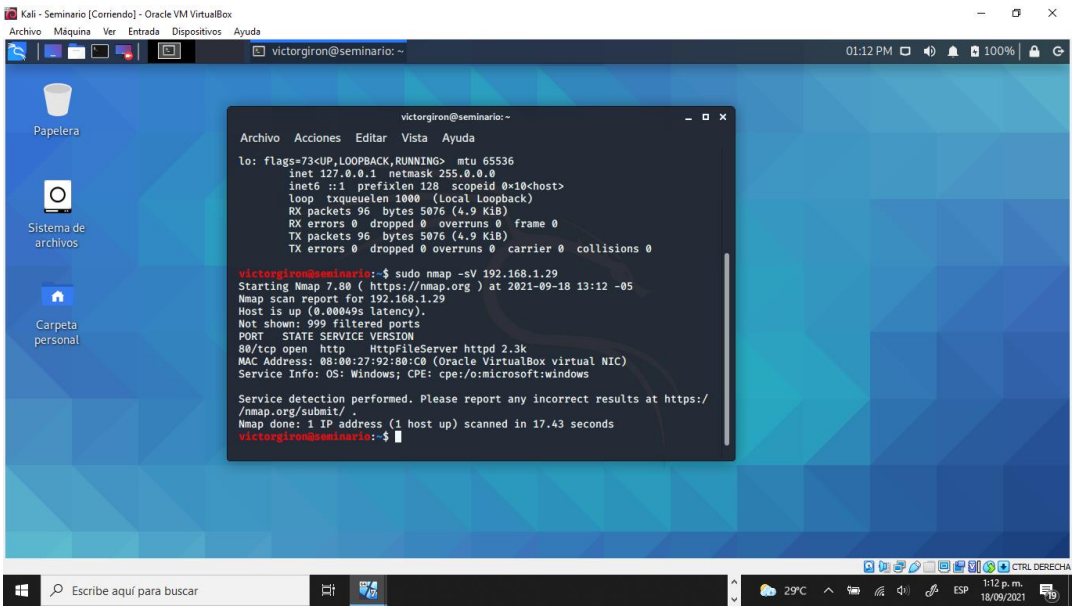
Figura 22: Elevación de privilegios al usuario creado en Kali Linux.



Fuente: Propiedad del autor.

Se vuelve a analizar la máquina de Windows 7con Nmap para encontrar la vulnerabilidad referente al programa “HtttpFileServer”, pero esta vez desde la cuenta “victorgiron” que hemos creado previamente.

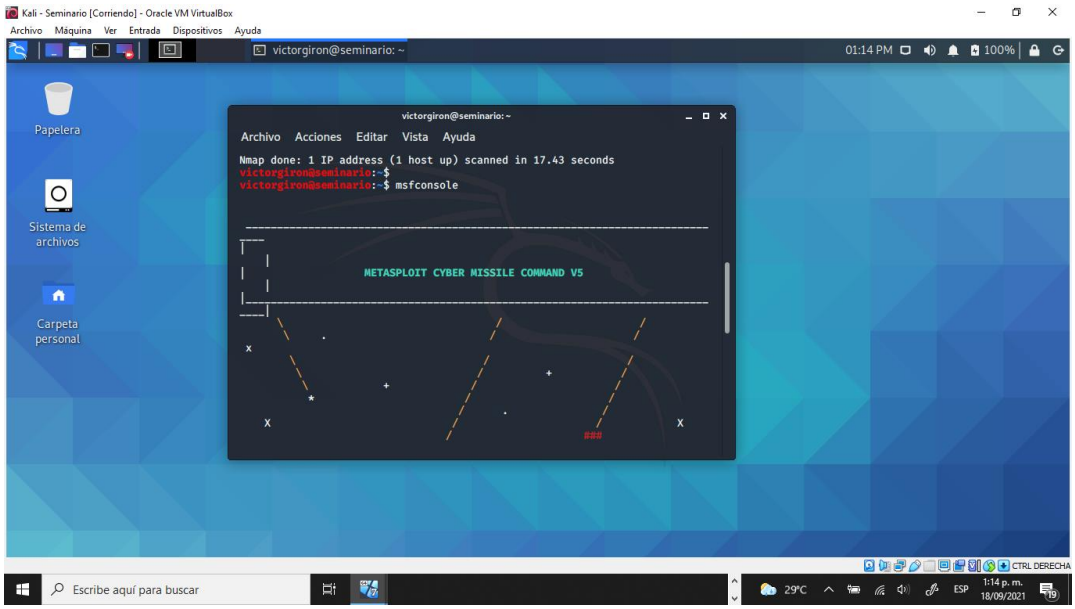
Figura 23: Escaneo de puertos en la maquina Windows 7 de 64 bits, desde Kali Linux.



Fuente: Propiedad del autor.

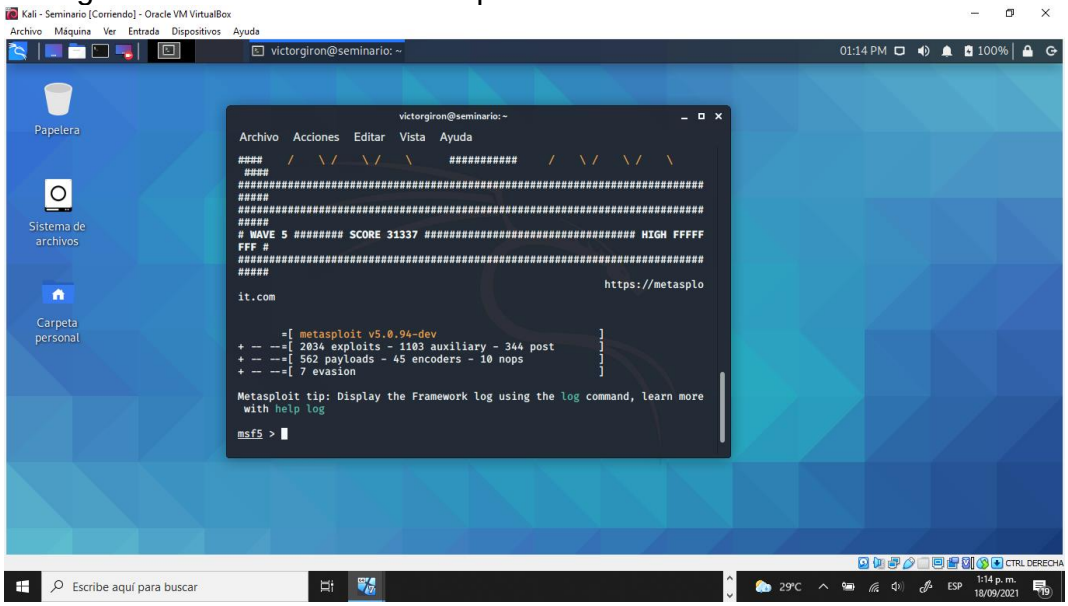
A continuación, se realiza la explotación de la vulnerabilidad encontrada por medio de un Metasploit ingresando a la consola, con el comando *“> msfconsole”*

Figura 24: Ingreso a la consola de Metasploit.



Fuente: Propiedad del autor.

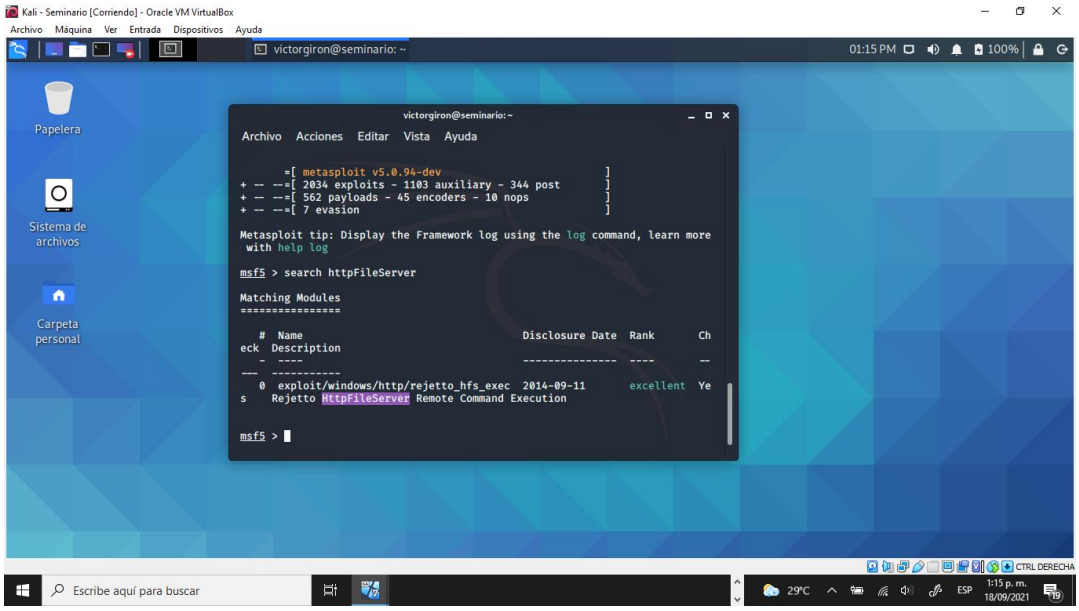
Figura 25: Ingreso a la consola de Metasploit.



Fuente: Propiedad del autor.

Se busca dentro del Metasploit el programa que está causando la vulnerabilidad con el siguiente comando: *"> search httpFileServer"*

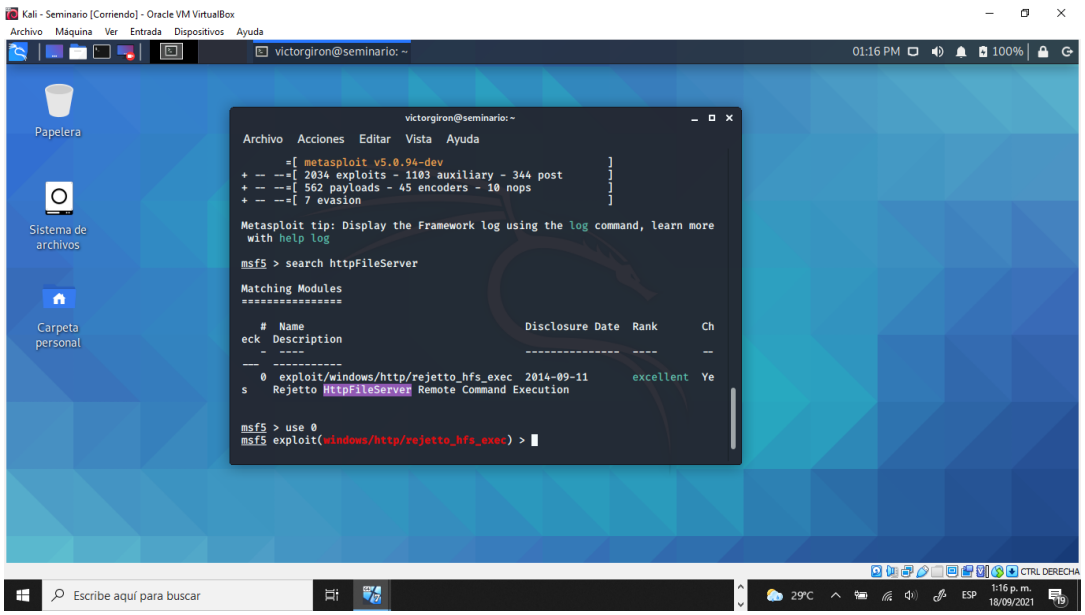
Figura 26: Búsqueda de “rejetto v. 2.3”.



Fuente: Propiedad del autor.

Se selecciona el módulo al cual le realizaremos el expliot, en este caso es el módulo cero (0), que es el único que aparece y se realiza con el siguiente comando *“> use 0”*

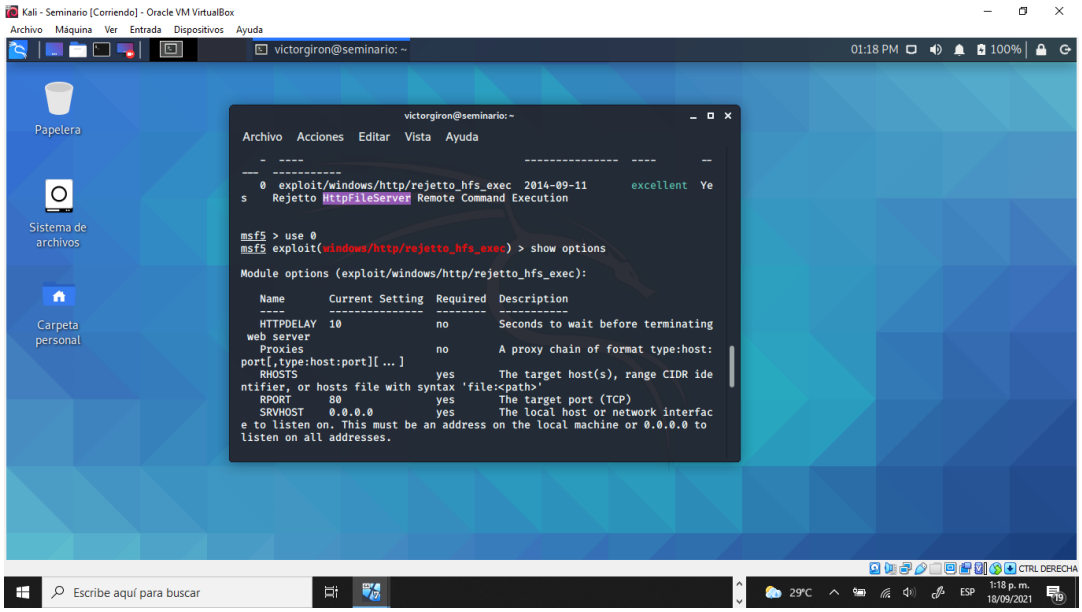
Figura 27: Selección de “rejetto v. 2.3”.



Fuente: Propiedad del autor.

A continuación, se miran las variables dentro del Metasploit para luego determinar cuál se utilizará en la explotación, en este caso se utiliza el comando “show options”

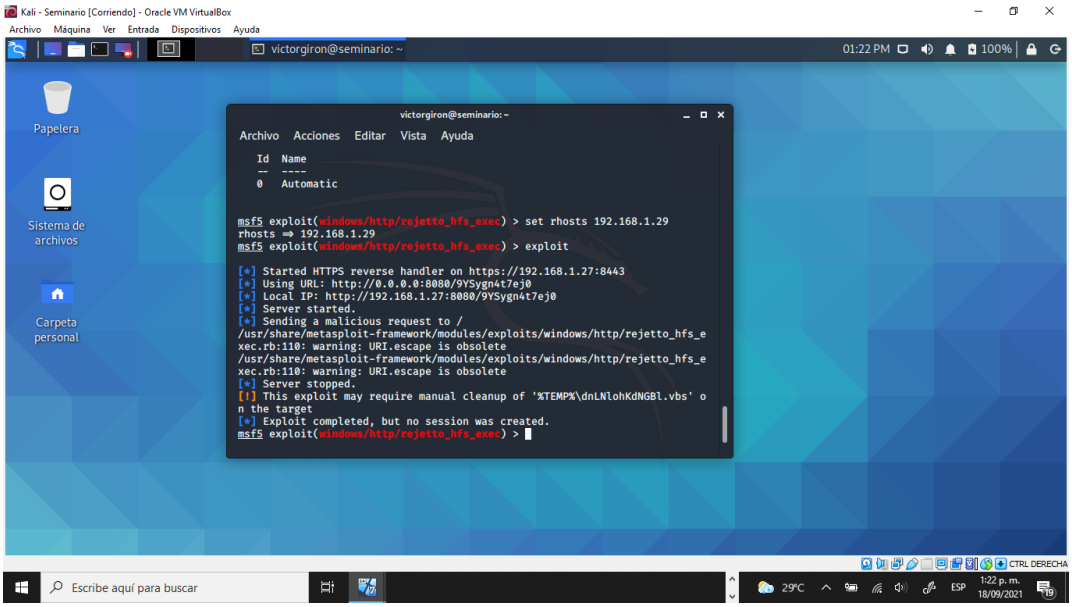
Figura 28: Variables del Metasploit.



Fuente: Propiedad del autor.

Y para realizar el ataque al sistema o máquina que tiene la vulnerabilidad se debe utilizar el comando “set” seguido del parámetro y el valor que se desea establecer, en este caso sería de la siguiente manera: *“> set rhosts 192.168.1.29”*

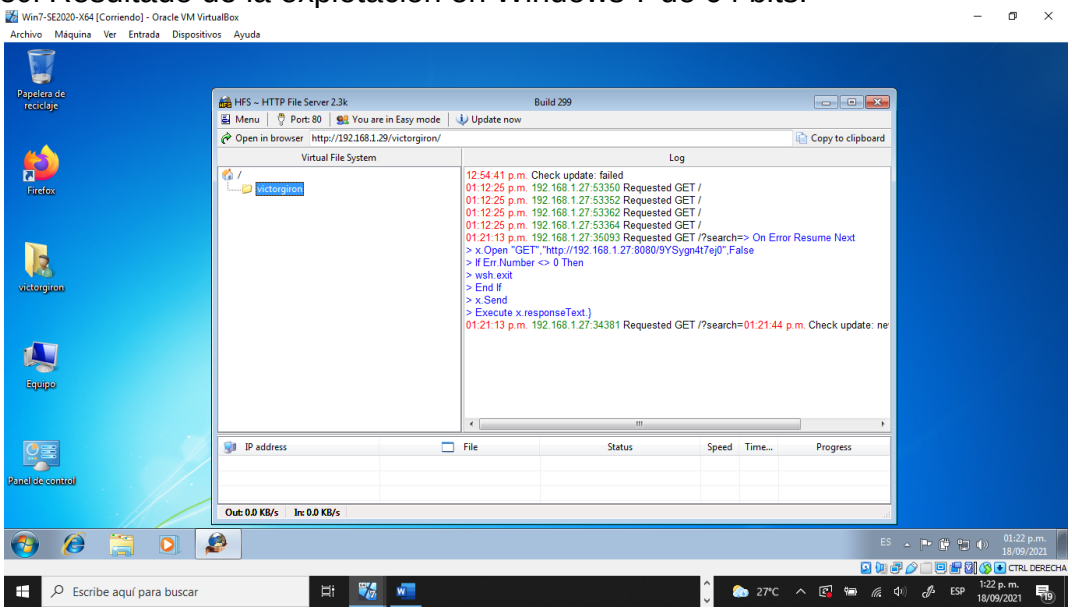
Figura 29: Explotación de la vulnerabilidad.



Fuente: Propiedad del autor.

En la máquina de Windows 7 donde se encuentra instalado el programa HttpFileServer podemos ver el resultado del ataque generado desde Kali Linux.

Figura 30: Resultado de la explotación en Windows 7 de 64 bits.



Fuente: Propiedad del autor.

Con esta prueba se puede determinar que se ha podido ingresar a la máquina de Windows 7 de 64 bist, se tuvo una respuesta remota por medio de la explotación de la vulnerabilidad y se tiene acceso a la maquina víctima.

Para el descubrimiento de la falla de seguridad para mi creo que lo importante fue que se estaba trabajando en un sistema el cual es obsoleto y que no se cuenta con las actualizaciones de seguridad instaladas, un sistema que ya perdió soporte técnico por parte del fabricante lo hace muy vulnerable. Lo otro que pienso es que el sistema tiene instalado una aplicación la cual me están informando de que tiene que está provocando una fuga de información y me están dando el nombre de la aplicación que los está generando y en este caso es “rejetto v 2.3, que está generando un exploit.

Las herramientas utilizadas en este análisis de la seguridad en dicho sistema operativo Windows 7 fueron las siguientes:

El sistema operativo Kali Linux, que es donde generamos el ataque a la máquina de Windows 7 de 64 bits por medio de la herramienta Metasploit, que es la que nos permite realizar el ataque y explotar la vulnerabilidad encontrada en la maquina cliente.

La herramienta de Nmap, se utiliza desde Kali Linux para la identificación de los puertos se encuentran abiertos en Windows 7 de 64 bits y poder identificar si la aplicación que tiene la vulnerabilidad tiene algún puerto asignado, y que en este caso es el puerto 80 y es por donde se podría acceder al sistema y cometer algún tipo de delito informático.

El puerto que abre la aplicación rejetto v. 2.3 es el puerto 80, es un puerto que por lo general se utiliza para publicar el sitio web que deseamos como un sitio estándar que utiliza el protocolo HTTP, el cual no es un protocolo seguro y que es más viable se sufran ataques a servicios web que tengan este tipo de protocolo.

La afectación de cualquier equipo de cómputo por medio de esta técnica dentro de una red de datos podría ser devastadora para una compañía o para cualquier persona que hace uso de las tecnologías de la informática, ya que esta técnica de explotación de vulnerabilidades de equipos o software se realiza en muchos de los casos sin que el usuario se dé cuenta, y sus ataques son efectivos pues muchos de los sistemas no cuentan o no les realizan actualizaciones de seguridad un factor determinante para confrontar los ataques cibernéticos.

Los pasos que se ejecutaron y sus respectivas evidencias para explotar la vulnerabilidad en la máquina Windows 7 de 64 bits fueron las siguientes:

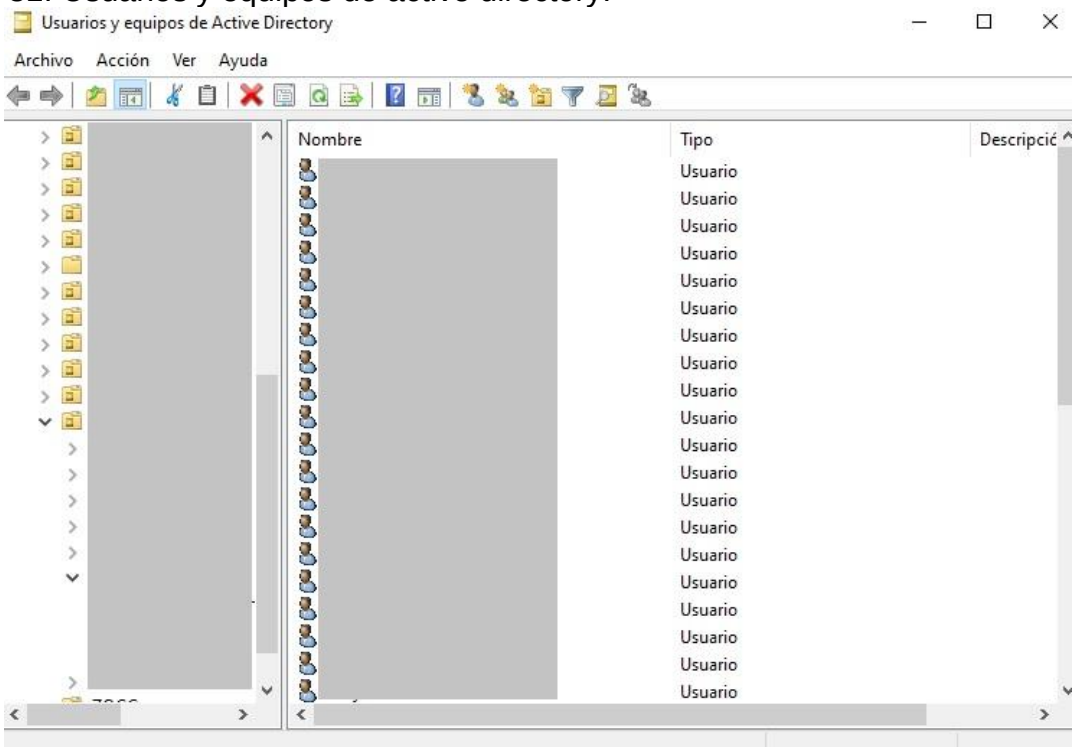
Se procede a instalar las dos máquinas virtuales tanto Kali Linux como Windows 7 de 64 bits, se crean los usuarios para realizar el proceso de análisis de vulnerabilidades y por ende la explotación de esta. Dentro del sistema de Windows 7 de 64 bits se desactiva el firewall y se crea un usuario con privilegios de administrador, con nombre “victorgiron” y dentro de Kali Linux igualmente se crea una cuenta de usuario con el mismo nombre “victorgiron”, desde el sistema de Kali Linux se analizan los puertos de la máquina de Windows 7 por medio del comando “Nmap”, nos arroja información importante con respecto al programa que está causando la fuga de información “rejetto v.2.3”, ya con esta información se procede a ejecutar el ataque desde Kali Linux por medio de la herramienta “Metaspliot”, por el cual nos determina que tenemos acceso a la otra maquina por medio del puerto 80.

6. CONTENCIÓN DE ATAQUES INFORMÁTICOS.

¿Teniendo en cuenta el ataque ejecutado desde el ejercicio de Red Team qué medidas de hardenización propondría para que el ataque no se repita?

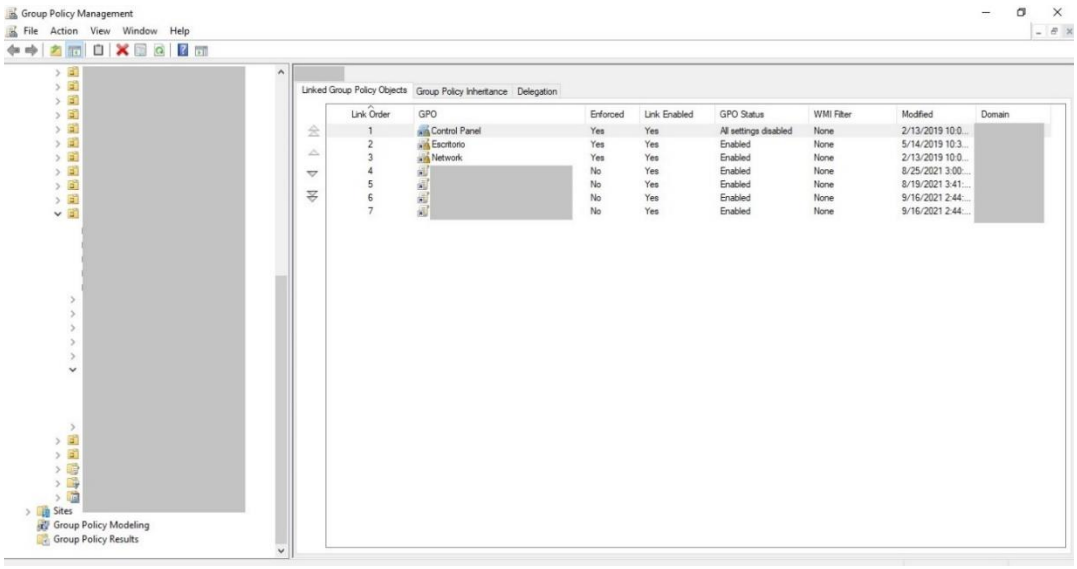
Las medidas que se pueden llegar a implementar para que el ataque no se repita son varias, teniendo presente el ataque ya visto con la máquina de Windows 7 de 64 bits. Estas medidas hacen referencia a todo lo que el usuario podría tener acceso dentro de la estación de trabajo, por ejemplo tener acceso a distintas particiones de disco duro, o si puede hacer uso de los puertos USB, son varias las medidas, pero si se quiere tener una seguridad robusta y que se puede implementar dentro de la compañía en mi caso utilizaría toda la configuración por medio del directorio activo en donde centralizaría todas las operaciones que realicen los usuarios de la organización por medio de la configuración de políticas de grupo, ya que es una muy buena herramienta que ayudaría a mantener una seguridad dentro del manejo de los recursos tecnológicos de la empresa.

Figura 31: Usuarios y equipos de active directory.



Fuente: Propiedad del autor.

Figura 32: Creación de políticas de dominio.



Fuente: Propiedad del autor.

Una vez determinada la medida a utilizar para endurecer el sistema de seguridad de la organización “WhiteHouse”, menciono a continuación que alternativas se podrían llevar a cabo dentro de esta:

- Configuraciones de las cuentas de usuario: Por ejemplo, que los usuarios acceden con cuantas de dominio limitadas que no tengan roles de administradores.
- Configuraciones de programas y aplicaciones: Que los usuarios solo puedan hacer uso de algunas aplicaciones al igual que navegadores de internet.
- Configuraciones de protocolos: Determinar que protocolos se usaran para el manejo de ciertos servicios dentro de la organización WhiteHouse, y los demás desactivarlos.
- Configuración de hardware: Determinar acceso a componentes como acceso de sistemas inalámbricos, acceso a puertos USB.
- Configuraciones de acceso remoto: Saber quiénes de los usuarios pueden tener acceso remoto y para que, este servicio es recomendable que no lo tengan todos los usuarios.

Las herramientas que podríamos mencionar son las siguientes:

Firewall Perimetral: Dentro de la administración de la red de datos, existen varias formas en las que se puede configurar una red de forma segura, en este caso se podría utilizar un Firewall perimetral, el cual tiene como función evitar que le red de la organización se comunique con una red externa a ella y que no cuente con la seguridad adecuada con respecto a las políticas de seguridad de la información de la organización. Con esta herramienta se logra que se analicen los paquetes de datos que ingresan a la red corporativa y bloquearlos según su información además de que una buena configuración de este Firewall Perimetral podría ayudar a determinar bloquear usuarios, movimiento de la red como el tráfico, entre otras opciones.

Servidor Proxy: Otra buena herramienta es la de un servidor proxy en la organización, con ella se logra la filtración de paquetes, bloqueo de sitios web que no sean prioritarios para la funcionalidad de la red dentro de la organización. Se limita quienes podrían tener acceso a la red externa y contar con informes de logs de ingresos o visitas a sitios ajenos a la institución.

Herramientas de escaneo de vulnerabilidades: Es una parte importante tener o contar con herramientas de escaneo de vulnerabilidades que ayuden a contener posibles riesgos en el sistema informático dentro de la organización, existen herramientas como lo son Wireshark, OpenVAS, OWASP, que vigilan la parte de software mirando cuales son los puntos débiles del sistema y como poder estar pendientes a un ataque generado por personal externo. En tiempo real se tiene resultados que hacen que se deba tomar medidas al instante sabiendo con certeza como se está afectando el sistema y como lograr recuperarlo u contrarrestar el ataque. Ahora bien, en el mercado existen sin número de aplicaciones sean de licencias pagas o GPL, solo resta identificar la que más se adapte las necesidades, mirar operatividad y los beneficios que aportan, realizar una buena configuración y así tener el sistema protegido pues lo más preciado para una compañía es su información y con tal de tenerla protegida no debería existir limitaciones de recursos en este aspecto.

7. ENLACE DEL VIDEO DE LA SOCIALIZACIÓN.

El video se encuentra en estas dos plataformas:

https://vimeo.com/627882831

https://youtu.be/BFEuxepqT4I

CONCLUSIONES.

Dentro de las conclusiones que se pueden plantear en el desarrollo de este informe técnico referente al análisis de riesgos y vulnerabilidades en una infraestructura tecnológica podemos mencionar lo siguiente.

Que dentro de cada país existen distintas normas y leyes a las cuales se está sujeto las personas que manejan u operan información de forma digital, por ello se debe documentar bien al momento de hacer uso de los sistemas informáticos y del manejo o trato de la información, ya que por desconocimiento de estas se puede incurrir en sanciones que perjudiquen las labores tanto personales como laborales. La invitación es a tener presente estas normativas, leyes, decretos para poder tener un buen manejo de la información y saber cómo defenderse cuando es víctima dentro del campo cibernético, esto ayudara afrontar los ataques, robos de información y operaciones técnicas en los sistemas computacionales.

Es importante decir que los principios éticos y morales son demasiado importantes para las personas como para las entidades o empresas que realizan un proceso de selección de personal. El deseo de construir una buena sociedad debe estar dentro de las políticas de las entidades sean públicas o privadas que la parte gerencial se comprometa con el bienestar social de sus empleados, y de allí poder fortalecer los relaciones con ellos haciendo que la empresa busque el beneficio en conjunto y que por ningún motivo se inmiscuya intereses individuales, ya que de ser así se tendrá el inicio del régimen autoritarito, podríamos decir que la parte delictiva siempre surgirá si no se tiene unos buenos principios morales sea en el escenario que sea.

Dentro del campo de las tecnologías de la información la delincuencia hoy en día ha tomado mayor auge en este campo, todas las operaciones ya se realizan de manera electrónica y las entidades deben contar filtros y sistemas más seguros que eviten la fuga de información que sin duda es lo más importante dentro de una organización, es el activo más preciado y que debe blindar y para eso debe contar con sistemas seguros que eviten con buenas herramientas de contención y a parte de un personal capacitado y comprometido con la seguridad de información, ser conscientes de que desde cualquier punto de la red a nivel global, alguien puede acceder al sistema y causar estragos, violar la seguridad de la red y tomar de forma remota el control de cualquier computadora sin que el usuario sé de por enterado, por eso es importante que las entidades inviertan en seguridad, que no escaseen recursos para ello que lo timen como unas de las prioridades de la empresa, de lo contrario es posible que en el futuro sufran constantemente ataques cibernéticos.

Y la contención de los posibles riesgos que dentro de una organización es muy importante, es una prioridad debido a que los activos de información en las entidades de hoy en día juegan un papel importantísimo para la misma entidad como para la competencia y personal externo a ella, es por eso por lo que buscar las medidas de protección siempre serán necesarias. Entre de las herramientas que

existen, es importante que existan distintas opciones para contar con una buena protección, no hay excusa para omitirla, y esto es un mensaje direccionado a la alta gerencia de las entidades, que prioricen la seguridad de sus organizaciones, que tengan muy presente que ya existen normas, decretos y leyes que les apoyan en el proceso y que cuando se tiene un respaldo de la información el trabajo dentro de ellas se realiza con mucha más convicción.

RECOMENDACIONES.

Se proponen algunas sugerencias que ayuden a mejorar la seguridad dentro de las compañías y que la haga ser más fuerte en caso de que llegara a presentar cualquier tipo de ataque cibernético.

Velar por el buen funcionamiento de la infraestructura tecnológica, realizar un buen uso de los equipos tecnológicos y llevar a cabo de la forma correcta todos los procesos de la organización teniendo presente la seguridad de la información.

Capacitar a todo el personal en temas de seguridad informática para complementar con la seguridad de la información.

Realizar auditorías permanentes para vigilar que los controles a los activos de información se estén realizando conforme a la política de seguridad de la información establecida por la organización.

Conformar dentro de la organización un grupo de equipos de Red Team y de Blue Team con el propósito de analizar la información en busca de vulnerabilidades y poderlas tratar oportunamente.

Contar con logs para el cual permita tener un control del acceso a los sistemas de la organización y poder validar si los usuarios que acceden a dichos sistemas son los correctos, de esta forma se pude mirar el comportamiento de los sistemas y programas con los que cuente la organización.

Deben realizar auditorías permanentes para realizar controles a los movimientos dentro de los sistemas de la organización y plantear políticas de seguridad internas.

Utilizar procesos de cifrado de datos dentro de la organización cuando sea posible, teniendo presente el tipo de información y el manejo al que esté relacionado.

Contar con sistema de protección de virus, de configuración de distintas herramientas como los firewalls y realizar periódicamente actualizaciones.

BIBLIOGRAFIA.

Catoira F. (2018). Pruebas de Penetración para principiantes: Explotando una vulnerabilidad con Metasploit framework. Consultado el 18 de septiembre de 2021. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

González P.P. (2019). Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux. Consultado el 18 de septiembre de 2021. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/91846/6/rmonterrozaTFM0119memoria.pdf

Ríos Yáguez, J. (2014). Técnicas y herramientas de análisis de vulnerabilidades de una red. Consultado el 18 de septiembre de 2021. Disponible en: https://oa.upm.es/32786/1/TFG_javier_rios_yaguez.pdf

Revista Seguridad. (2018). Pruebas de penetración para principiantes: Explotando una vulnerabilidad con Metasploit Framework | Revista. Seguridad. Consultado el 14 de septiembre de 2021. Disponible en: https://revista.seguridad.unam.mx/numero-19/pruebas-de-penetraci%C3%B3n-para-principiantes-explotando-una-vulnerabilidad-con-metasploit-fra

Incibe. (2014). OWASP Testing Guide v4.0. Guia de seguridad en aplicaciones Web. INCIBE-CERT. Consultado el 14 de septiembre de 2021. Disponible en: https://www.incibe-cert.es/blog/owasp-4

Incibe. (2019). ¿Qué es el pentesting? Auditando la seguridad de tus sistemas. INCIBE. Consultado el 14 de septiembre de 2021. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/el-pentesting-auditando-seguridad-tus-sistemas

RSI Security. (2020), ¿QUÉ ES EL CENTRO PARA LA SEGURIDAD DE INTERNET (CIS)? Consultado el 27 de septiembre de 2021. Disponible en: https://blog.rsisecurity.com/what-is-the-center-for-internet-security-cis/

INTELEQUIA (2021). RED TEAM Y BLUE TEAM - FUNCIONES Y DIFERENCIAS EN CIBERSEGURIDAD. Consultado el 25 de septiembre de 2021. Disponible en: https://intelequia.com/blog/post/2088/red-team-y-blue-team-funciones-y-diferencias-en-ciberseguridad

SOFECON. SIEM, la tecnología capaz de detectar y neutralizar las amenazas informáticas antes de que ocurran. Consultado el 25 de septiembre de 2021. Disponible en: https://sofecom.com/que-es-un-siem/

Gómez, L. & Álvarez, A. (2012). Introducción y comprensión a los sistemas de gestión de seguridad de la información SGSI (ISO/IEC 27001-27002): Guía de

aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. (pp. 13-34, 45-47). Consultado el 29 de septiembre de 2021. Disponible en: https://bibliotecavirtual.unad.edu.co:2538/lib/unadsp/reader.action?ppg=13&docID=3205110&tm=1543960307637

ISO 27001. (2019). El portal de ISO 27001 en español. Consultado el 30 de septiembre de 2021. Disponible en: http://www.iso27000.es/

Webescolar. (2010). Funciones de control interno y auditoría informática. Consultado el 29 de septiembre de 2021. Disponible en: https://www.webscolar.com/funciones-de-control-interno-y-auditoria-informatica

Chicano, E. (2015). Auditoría de seguridad informática. Consultado el 30 de septiembre de 2021. Disponible en: https://books.google.com.co/books?hl=es&lr=&id=8a3KCQAAQBAJ&oi=fnd&pg=PT4&dq=auditoria+informatica&ots=ja4mIHS5Pt&sig=m-2Ns7iR32H6oRiZCMaK04TwVnY&redir_esc=y#v=onepage&q&f=false

Cortes, D. (2017). El proceso de Auditoria Informática. Consultado el 30 de septiembre de 2021. Disponible en: https://www.seguridadyfirewall.cl/2017/01/el-proceso-de-auditoria-informatica.html

Securityartwork, A. Huerta (2012), Introducción al análisis de riesgos – Metodologías (II). Consultado el 01 de octubre de 2021. Disponible en: https://www.prakmatic.com/gestion-ti/metodologias-de-gestion-ti-para-mejorar-tus-proyectos-empresariales/

Solarte, F. N. J. (2016). Sistema de gestión de seguridad de la información SGSI bajo la norma ISO 27001 y 27002. Consultado el 01 de octubre de 2021. Disponible en: http://sgsipractico.blogspot.com.co

Solarte, F. (Productor). (2016). Metodología de gestión de riesgos de seguridad informática. Consultado el 01 de octubre de 2021. Disponible en: http://hdl.handle.net/10596/10742

Li, Zhen and Zou, Deqing and Xu, Shouhuai and Ou, Xinyu and Jin, Hai and Wang, Sujuan and Deng, Zhijun and Zhong, Yuyi (2018). VulDeePecker: A Deep Learning-Based System for Vulnerability Detection. Consultado el 02 de octubre de 2021. Disponible en: https://arxiv.org/pdf/1801.01681.pdf

M. Junjin, (2009). "An Approach for SQL Injection Vulnerability Detection," Sixth International Conference on Information Technology: New Generations, 2009, pp. 1411-1414, doi: 10.1109/ITNG.2009.34. Consultado el 02 de octubre de 2021. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5070824

ISO/IEC 27001:2013 — Informationtechnology — Security techniques — Informationsecuritymanagementsystems — Requirements (secondedition).

Consultado el 01 de octubre de 2021. Disponible en: https://www.iso27001security.com/html/27001.html

F. Wu, J. Wang, J. Liu and W. Wang (2017). "Vulnerability detection with deep learning," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017, pp. 1298-1302, doi: 10.1109/CompComm.2017.8322752. Consultado el 02 de octubre de 2021. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8322752

J. Jeremiah, (2019). "Intrusion Detection System to Enhance Network Security Using Raspberry PI Honeypot in Kali Linux," International Conference on Cybersecurity (ICoCSec), 2019, pp. 91-95, doi: 10.1109/ICoCSec47621.2019.8971117. Consultado el 04 de octubre de 2021. Disponible en: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8971117

Vijay Kumar Velu, Robert Beggs (2019). Mastering Kali Linux for Advanced Penetration Testing. Consultado el 04 de octubre de 2021. Disponible en: https://books.google.es/books?id=kQGGDwAAQBAJ&lpg=PP1&ots=N0tID157zm&dq=vulnerability%20detection%20kali%20linux&lr&hl=es&pg=PP1#v=onepage&q=vulnerability%20detection%20kali%20linux&f=false

Gonzales Cotera, Bernier (2017). USO DE HERRAMIENTAS DE ETHICAL HACKING CON KALI LINUX PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA SEDE CENTRAL DE LA UNIVERSIDAD DE HUÁNUCO. Consultado el 04 de octubre de 2021. Disponible en: http://repositorio.udh.edu.pe/bitstream/handle/123456789/675/GONZALES%20COTERA%20BERNIER.pdf?sequence=1&isAllowed=y

Quirumbay Y. D. (2021). Análisis de amenazas y vulnerabilidades informáticas basado en la Norma ISO 27002, en el proceso de citas del servidor web de una Institución. Consultado el 04 de octubre de 2021. Disponible en: https://repositorio.upse.edu.ec/bitstream/46000/5754/1/UPSE-TTI-2021-0007.pdf